TS-01-0003

科来网络分析系统 6.4

产品使用手册

技术支持部
科来软件
电话：86-28-85120922
传真：86-28-85120911
网址：http://www.colasoft.com.cn
邮件：support@colasoft.com.cn

目　录

一．产品概述

科来网络分析系统是一个集数据包采集、解码、协议分析、统计、日志图表等多种功能为一体的综合网络分析系统。它可以帮助网络管理员进行网络监测、定位网络故障、排查网络内部的安全隐患。

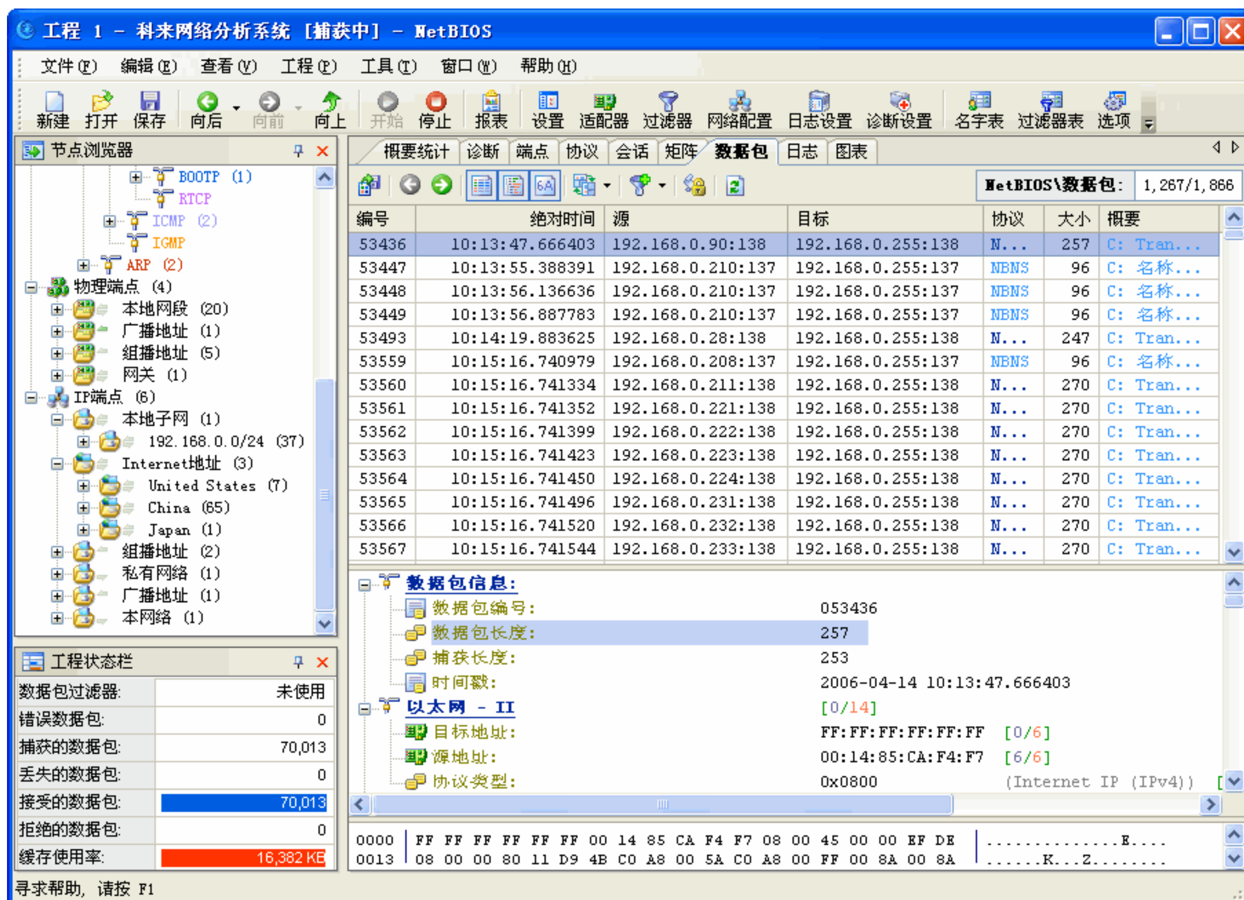
科来网络分析系统能够进行全实时的采集-分析-统计处理，能够即时的反应网络通讯状况，不需要进行任何后期处理。

科来网络分析系统强大的数据包解码功能可以让最为狡猾的网络攻击、欺骗行为也无所遁形；针对常用网络协议设计的高级分析模块为用户提供更为实用的网络使用数据记录；网络通讯协议和网络端点都可以提供详尽的数据统计；独创的协议、端点浏览视图结构，可以帮助用户快速定位所要数据；丰富的图表功能为用户提供直观的信息。

不管是本地局域网的诊断还是到大型网络的监测，科来网络分析系统都是一款不可或缺的网络管理工具。有了这样的工具，可以帮助企业网络完成以下几类工作：

- 网络流量分析
- 网络通讯监视
- 网络错误和故障诊断
- 网络安全分析
- 网络性能检测
- 网络协议分析

网络分析工具的配备可以从本质上检测到网络中的问题，协调和支持各种网络管理工具的使用，并最大化的完善网络管理。



1. 版本信息

科来网络分析系统 6.4 包含三个版本：专业版、企业版、专家版。

下面的对比表主要显示两个版本的对比：

版本 / 功能	专业 Professional Edition	企业版 Enterprise Edition	专家版 Expert Edition
数据采集以太网方式	√	√	√
本地环回方式	X	√	√
概要统计	√	√	√
端点统计	√	√	√
协议分析	√	√	√
连接(会话)分析	√	√	√
数据包解码分析	√	√	√
日志记录	√	√	√
支持的网卡数	一个网卡	多网卡支持	多网卡支持
过滤器	简单过滤器	简单/高级过滤器	简单/高级过滤器
网络配置	X	√	√
网络快照	X	√	√
图表功能	X	√	√
报表功能	X	√	√
节点活动监视	X	√	√
专家诊断系统	X	X	√

矩阵功能（新）	✗	✗	√
数据包播放（新）	✗	✗	√
PING 管理 CPING（新）	✗	✗	√
MAC 扫描 CMAC（新）	✗	✗	√
上网控制 CSIAB（新）	可选	可选	可选

2. 使用许可协议

本协议是您(个人或单一实体)与科来软件之间关于使用科来网络分析系统的法律协议，请认真阅读。

本协议适用于科来网络分析系统 6.4 版本。软件包括计算机软件，并可能包括与之相关的媒体和任何的印刷材料，以及联机的电子文档（下称“软件产品”或“软件”)。一旦安装、复制或以其他方式使用本软件产品，即表示同意接受协议各项条件的约束。如果您不同意本协议的任一条款，则不能获得使用本软件产品的权力。

版权

科来软件（以下简称“科来软件”)自 2003 年开始拥有科来网络分析系统的版权。本软件的使用和版权受中华人民共和国法律和国际版权条约和其他知识产权法及条约的保护。用户获得的只是本软件产品的使用权，科来软件保留本软件及其相关文档的全部权利，所授予的任何许可都不能有损于此项权利。您不允许以文字，电子或者其他任何形式重新传播提供给您的授权文件。

企业使用许可

个人购买只允许由被授权人所使用，他/她只能将软件安装到指定的一台电脑上。

企业用户购买本产品，允许授权人将产品安装在授权企业的一台或多台电脑上。但不得泄露、出售、授权或以其他方式传播产品，如果该产品的授权信息被其它非授权企业使用，将被视为非法传播，授权企业需要承担相应责任。

被授权人不可以转让软件许可，必须同意本软件许可协议规定的条款和条件。

免责条款

使用本软件产品由用户自己承担风险。科来软件不提供任何明示的或是暗示的担保，包括但不限于对产品的担保和适用于特定目的的担保。在任何情况下，即使预见到产生这种损失的可能性，科来软件对您的任何损失，包括偶然性损失或因使用本软件产品而导致的结果性损失，都不承担责任。您应确认已仔细阅读过此许可协议并充分理解其含义，而且同意受本协议条款的约束。

法律管辖

本协议受中华人民共和国管辖。

传播

您可以传播本软件产品的 Demo 版本，但必须包括全部的原始文件。但是为盈利目的而传播本软件产品时，必须事先与我们联系并取得授权。

科来软件不允许您泄露、出售、授权或以其他方式转播本软件产品的完整版本。

其他限制

您不得以任何方式：

删除本软件及其他副本上一切关于版权的信息；

销售、出租此软件产品的任何部分；

制作和提供本软件的授权文件和破解程序；

对本软件进行反向工程，如反汇编、反编译等。

如果您没有遵守本协议的任一条款，科来软件有权立即终止本协议，且您必须立即终止使用本软件产品并销毁本软件产品的所有副本。

使用盗版的本软件产品的一切后果由使用者自己承担。对于使用盗版的本软件产品对使用者的操作系统造成的损害，科来软件及其代理商不承担任何责任。

3. 购买信息

购买：
如果您需要购买产品，或了解产品购买的相关信息，请与我们的联系：sales@colasoft.com.cn。
或访问我们的网站获取更多的购买信息： http://www.colasoft.com.cn/purchase/
目前，我们为您提供两个版本以供选择：专业版和企业版，您可以查看版本比较。

产品附件：
产品外包装盒，CD 盒，产品光盘，用户信息卡，用户手册。

4. 服务与技术支持

产品服务

我们为用户提供完善的售前和售后服务，让用户放心使用我们产品。

售前服务：
1）产品咨询 – 了解用户需求，并提供解决方案，向用户正确介绍产品的功能以及使用。
2）提供试用 -- 向用户提供产品试用，并进行技术指导。

售后服务：
1）技术支持 – 为用户提供产品的技术咨询和使用解答。
2）升级服务 – 为正式用户提供一年的免费升级。
3）故障处理 – 通过远程技术或故障报告，指导用户排除故障。

技术支持

注意：
只有授权用户才有权获得技术支持服务。

一般的问题，请先参阅本产品的 FAQ 与使用技巧。如果在使用本系统时遇到问题而参阅帮助文件仍不能解决的，请您联系当地的代理商以获取更多建议，或者选择以下方法从科来公司获得技术支持：

网站技术支持
从我们的网站上找到解决您问题的方法：http://www.colasoft.com.cn/support/
除了常见问题和术语表，我们还为您提供版本升级信息和与本系统有关的公共资源信息。

电子邮件技术支持
任何时候我们都欢迎您用电子邮件告知我们您遇到的问题，我们将尽快回复。请在邮件中注明您的产品序列号、产品版本、操作系统类型、详细的问题描述和其它相关信息。Email：support@colasoft.com.cn。

传真技术支持
紧急情况下要获得快速解决方案， 您可以发传真到 028－85120911 与我们联系。请在传真时注明您的产品序列号、产品版本、操作系统类型、详细的问题描述和其它相关信息。

电话技术支持
欢迎您致电咨询解决方案。除节假日以外，您都可以在每天上午 9 点至下午 5 点通过电话联系我们：028－85120922。

二．功能与特性

科来网络分析系统 6.4 对产品做了重大的改进，同时也增加了许多新的功能。以下是一些重要功能与特性，您也可访问我们的网站，要了解产品的最新功能，http://www.colasoft.com/products/capsa.php.

1. 会话视图

这是科来网络分析系统 6.4 版本新增加的一个功能，提供物理地址、IP 地址、TCP 连接、UDP 会话的通讯情况，通过查看会话，可以统计出其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。

2. 矩阵视图

这是科来网络分析系统 6.4 版本新增加的一个强大的功能。矩阵视图可对网络中通讯的节点和会话进行详细统计，通过统计我们可了解到整个网络通讯的节点/会话信息、某台物理主机/IP 主机的通讯节点/会话信息、以及某条会话的主机信息

3. 专家诊断

专家诊断是一个完成智能化的故障诊断功能，也是 6.0 有特色的一个功能，该功能可以按事故等级，实时提供每个网络层的错误和故障问题，分析故障原因并准确定位到故障点，提供故障的产生原因和专家

建议，将大大提高管理人员的网络事故的分析效率，大幅降低故障处理时间。

4. 数据查找

这是 6.0 版本的一个强大功能，用户可以在统计的数据中，根据指定的数据来查找统计结果，这将大大节省数据查找时间，便于用户快速分析网络数据。此功能可应用到"节点浏览器"、"端点分析"、"协议分析"、"会话分析"、"数据包分析"、"数据流分析"、"日志分析"等。

5. 统计分析

科来网络分析系统 6.4 提供了全新的统计分析，新的统计分析包含三大部份：概要统计、端点统计、协议统计、图表统计。这些统计可以帮助您了解整个网络的使用状态，包括流量的使用，数据包的分析，网络中的服务应用比例，带宽占用等。同时，也可以让您实时监测网络中的各种错误数据，如：CRC 错误包，802.3 错误，数据包冲突次数等。 要了解统计分析的更多信息，请查看 " 统计分析介绍 " 。

6. 图表统计

图表功能为用户提供 2D 或者 3D 的时间趋势图和数据比较图，可以选择折线图、柱状图、面积图、饼图等多种形式，除了全局图表，也支持每个协议和网络端点的图表数据采集显示。 用户可以通过采集时间来放大缩小网络历史数据的范围，也可以采用图表对比模式，对比同一节点的不同图表统计。了解图表统计的更多内容，请查看 " 图表介绍 " 。

7. 报表

您可以随时将网络统计分析结果生成一个完整的报表。报表以网页方式展示每个视图中的重要信息，在生成报表之前，用户可以调整统计图的显示样式。请查看 " 报表 " 的详细介绍。

8. 打印和打印预览

在每个分析视图中，用户都可以选择感兴趣的数据进行打印；我们同时也为用户提供打印预览功能，在打印之前，用户可以对将要打印出的效果进行查看。

9. 支持更多协议

协议层	支持协议
Application	BGP, BOOTP, CIFS, DHCP, DNS, Finger, FTP, FTP Control , FTP Data, Gopher, H.323, HTTP, HTTPS, IMAP, IMAP3, IMAPS, IPv6, LDAP, LDAPS, Mobile IP, MSN, NFS, NNTP, NTP, POP2, POP3, POP3s, HTTP Proxy, RLOGIN, RTSP, SLP, SMB, SMTP, SNMP, Telnet, TFTP，QQ，Bit Torrent
Presentation	AFP, Datagram Service, Name Service, NCP, NetBIOS
Session	RPC, SAP, Session Service
Transport	H.225, RTCP, SSH, TCP, UDP, NetBEUI
Network	CGMP, EIGRP, EGP, GRE, ICMP, ICMPv6, IGMP, IGRP, IP, IP Fragment, IPX, OSPF, PIM, RSVP, VRRP,RIP,rRIPv1,RIPv2,RIPv3,RIPv4
Data Link	ARP, Ethernet II, Ethernet 802.2, Ethernet 802.3, Ethernet SNAP, PPPoE, RARP, STP, VLAN
Others	Kerberos, GTP， L2TP, LPD, MGCP, MSRDP, MSSQL, PPTP, RSH, RTELNET, SCTP, SQL,SIP, WhoIs, WINS, AH, ESP, PUP, CDP

科来网络分析系统 6.4 支持几乎所有的常用协议，包括 RADIUS，RTSP，SOCKS，NetBIOS，RPC，ARP，IGRP 等等。这些协议的支持，可以让用户更清楚网络带宽的分配情况。

要了解更多的支持协议，请查看产品网站上的产品规格表。

10. 命令行支持

您可以通过命令行来启动或关闭科来网络分析系统，这对定制自动服务是非常有用的；除此之外，您可也可通过命令行参数打开一个工程文件，决定什么时候运行什么时候停止等，请查看“命令行”介绍。

11. 名字表

名字表包含 IP 地址表、MAC 址表和端口对应表，用户可以通过名字表对网络中的地址或端口进行定义，方便网络管理，增强数据可识别性，请查看“名字表”的详细介绍。

12. 统计快照

由于监测和统计分析都是实时进行的，网络的分析数据在不断更新，为了保留某一时刻的数据信息，可以通过快照功能，把当前的统计分析信息拍下来，便于数据对比和详细分析。 快照功能支持 10 次记录显示，您也可以删除不需要的快照。

13. 数据包摘要解码

摘要分析向管理人员提供数据包的概要信息，或重要分析结果，主要包括：数据包被捕获的绝对时间、源 IP 及使用端口、发送的目标 IP 及端口、使用的协议、数据包的大小、概要内容等。你也可以对摘要信息中重要的数据包进行标记，以便以后查看它们。

要了解数据包概要解码的应用，请查看“数据包概要解码”的详细信息。

14.强大的日志功能

日志功能包括四个基本的应用日志：HTTP，FTP，Email，DNS。用户可以分别保存这些日志文件，也可以打开通过 Email 发送和接收的邮件。

要了解日志分析的应用，请查看“日志”功能的详细介绍。

15.强大的过滤

科来网络分析系统的过滤器由简单过滤与高级过滤器组成；在应用时，管理人员可以根据需要使用过滤器对数据进行分离，这样可以丢弃无关的数据，便于对特定数据的监测，同时也提高分析效率。

科来网络分析系统提供了一个默认的过滤器列表。这些过滤器都是以按照协议为条件的过滤器，每个过滤器都可以使用“接收”和“排除”来指定其过滤条件。也可以随意组合其中的过滤器来制定数据包的捕获范围。要了解过滤器的更多信息，请查看“过滤器”的详细内容。

16.定位节点

通过数据分析时，可很容易的定位产生数据的节点，是哪个 IP 地址或物理地址；也可以定位于是哪一种网络协议。这样便于从微观到宏观的数据分析，对数据的关联查找，数据比较是非常有用的。

17.支持多网卡同时分析

在实际应用中，你的管理电脑可能会安装多网卡(network interface cards -- NICs)，那么，可以使用科来网络分析系统同时对多个网卡的数据进行分析；也可以采用不同的工程分别对每个网卡进行数据分析，请参见“工程设置 - 网络适配器”的详细信息。

18.高级分析模块

除了基本的数据分析模块外，科来网络分析系统还支持四种高级分析模块：Email 分析模块，FTP 高级分析模板，HTTP 高级分析模块，DNS 高级分析模块。这些高级分析模板都支持 TCP 数据流的重组功能，将网络中采集到的信息还原成为邮件，FTP 传输和访问的网站链接。请查看“高级分析模块日志”的详细信息。

19.支持本地环回

在启动某种应用时，如果客户端和服务器端都是主机自己，那么，客户端和服务器端之间的访问并不经过网卡，要对这部份的流量分析，就需要分析工具支持本地环回功能。请参见“工程设置 - 网络适配器”的详细信息。

20.相关数据包

在数据包分析时，你可以通过数据包的某个特征值，把其它相关的网络数据包全部关联出来。请查看“数据包解码 - 概要解码”的详细内容。

21.节点浏览器

节点浏览器最大的用途，就是能快速的选择需要查看的节点，通过选择节点，用户可以查看该节点对应的网络数据。节点浏览器由三个类组成，分别是协议节点，物理节点，IP 节点。用户可以很方便的定位到整个网络，也可以定位到某个 IP 段，或是某个 IP。而右边的数据会根据选择的节点显示相关的数据，科来网络分析系统 6.4 的节点浏览器还可以显示当前节点通讯状态。请查看“节点浏览器” 的详细内容。

22.工程状态栏

我们为每个工程都提供一个状态栏，用户可以查看当前工程的执行情况和配置状态。包括使用的过滤器，捕获到的数据包，数据包缓存的占用情况等。请查看“工程状态栏”的详细内容。

工程状态栏

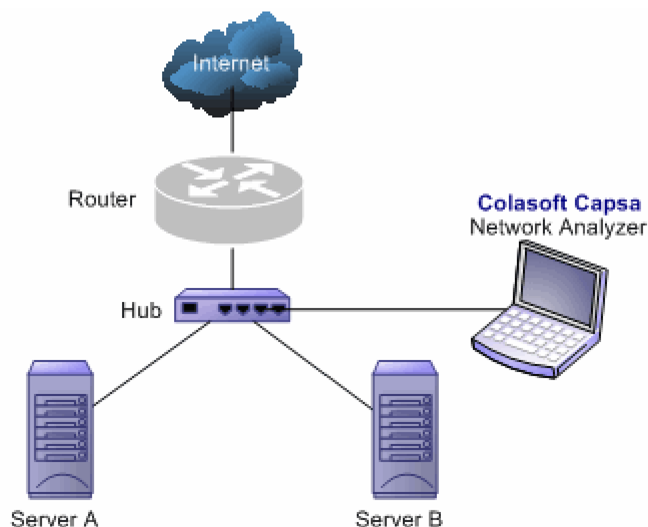
数据包过滤器:	未使用
错误数据包:	0
捕获的数据包:	908,280
丢失的数据包:	0
接受的数据包:	908,280
拒绝的数据包:	0
缓存使用率:	16,383 KB

三．产品部署说明

科来网络分析系统可以进行内网以及内网与外网的数据检测分析，甚至可以跨 VLAN 进行数据监测。只安装在一台管理机器上即可，不用安装到局域网的每台机器。管理人员可以根据需要，来决定网络的安装位置，安装位置的不同，捕获到的网络数据也差异很大。为了更全面的监测网络数据，我们建议最好将产品部署的设备直接连接到中心交换设备上，这样可以更多的数据信息；您也可利用网络分接器，来分析任意网段的数据。下面我们介绍几种常见产品部署。

1. 共享网络 - 通过 Hub 连接上网

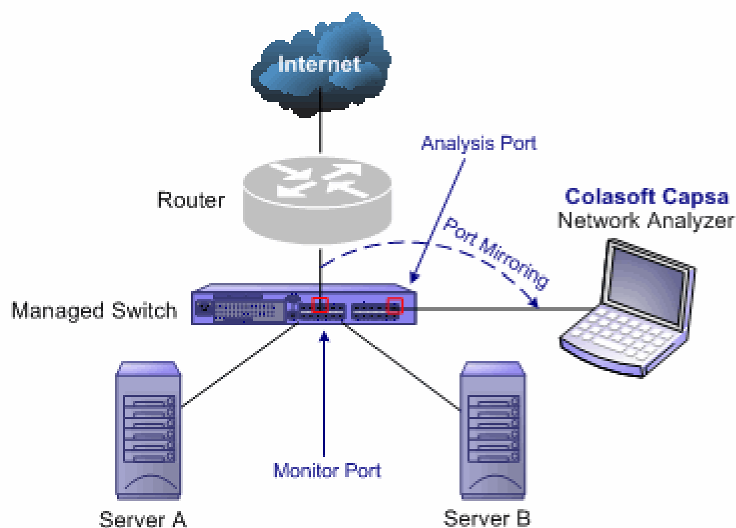
使用集线器（Hub）作为网络中心交换设备的网络即为共享式网络，集线器（Hub）以共享模式工作在 OSI 层次的物理层。如果您局域网的中心交换设备是集线器（Hub），可将科来网络分析系统可安装在局域网中任意一台主机上，此时科来网络分析系统可以捕获整个网络中所有的数据通讯。



2. 交换式网络 - 交换机具备管理功能（端口镜像）

使用交换机（Switch）作为网络的中心交换设备的网络即为交换式网络。交换机（Switch）工作在 OSI 模型的数据链接层，交换机各端口之间能有效地分隔冲突域，由交换机连接的网络会将整个网络分隔成很多小的网域。

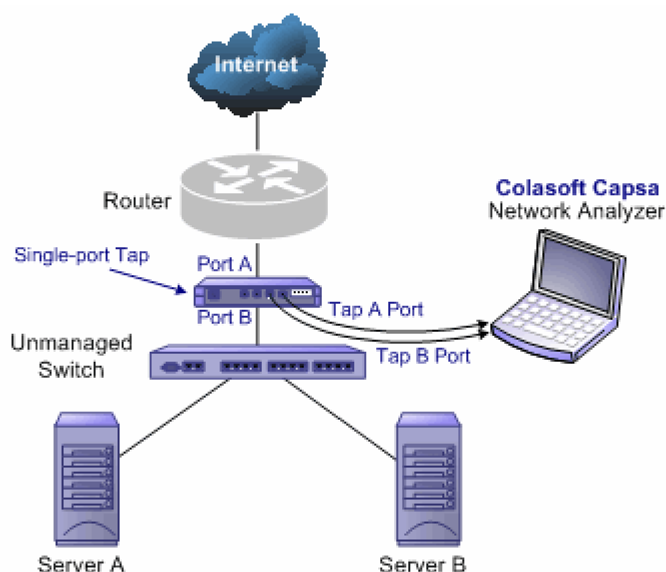
大多数三层或三层以上交换机以及一部分二层交换机都具备端口镜像功能，当您网络中的交换机具备此功能时，可在交换机上配置好端口镜像（关于交换机镜像端口），再将科来网络分析系统可安装在连接镜像端口的主机上即可，此时科来网络分析系统可以捕获整个网络中所有的数据通讯。



3. 交换式网络 - 交换机不具备管理功能（端口镜像）

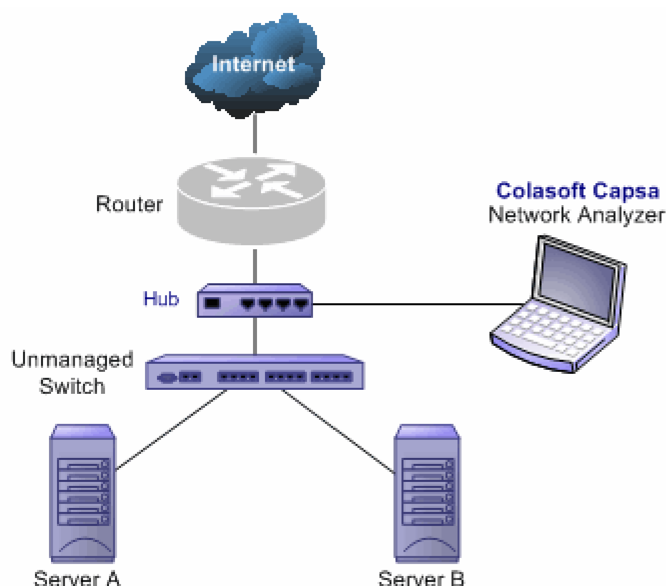
一般简易型的交换机不具备管理功能，不能通过端口镜像来实现网络的监控分析。如果您的中心交换或网段的交换没有端口镜像功能，一般可采取串接集线器（Hub）或分接器（Tap）的方法进行部署。如图所示：

使用网络分接器(Taps)
使用 Tap 时，成本较高，需要安装双网卡，并且在管理机器不能上网，如果要上网，需要再安装另外的网卡。



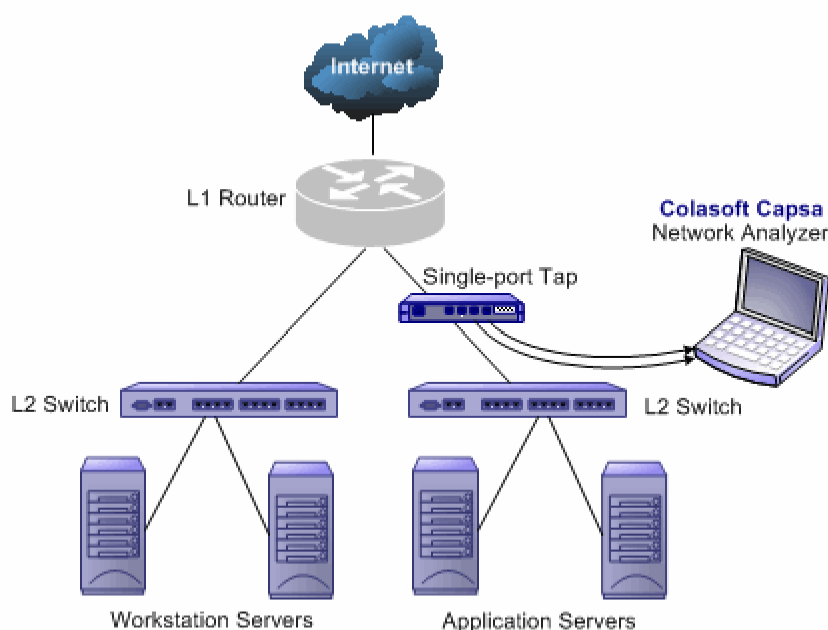
使用集线器(Hub)
Hub 成本低，但网络流量大时，性能不高，Tap 即使在网络流量高时，也对网络性能不会造成任何

影响，



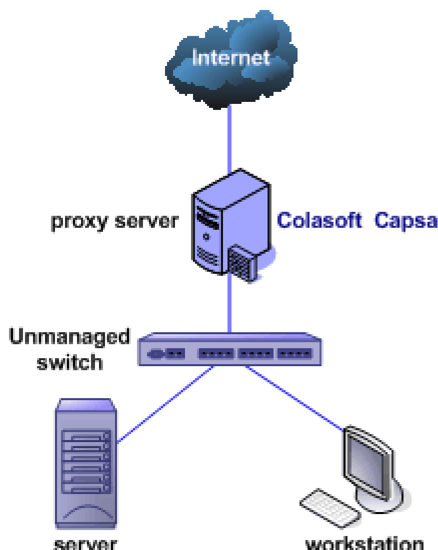
4. 定点分析某个网段

在实际情况中，网络的拓扑结果往往非常复杂，在进行网络分析时，我们并不需要对所有的网络进行分析，而只需要对异常的网段进行监测。对于这种情况，我们建议您将产品安装于移动电脑上，再附加一个网络分接器，就可以很方便的来检测任意链路上的网络情况。



5. 使用代理服务器

当前的小型网络中，有很大一部分都通过代理服务器共享上网。这里我们根本没有以上几种情况下的分析用笔记本，而是将科来网络分析系统直接安装在代理服务器上。



6．使用集线器 Hub、分接器 TAP、交换机 Switch 的区别？

	集线器 Hub	交换机镜像 Mirror Port	网络分接器 TAP
优点	成本低 不需要进行配置 无需改变网络原有拓朴结构	不需要增加额外设备 无需改变网络原有拓朴结构	对网络传输性能无任何影响。 不干扰数据流，对结果无影响。 不占用 IP，不受网络攻击 无需改变网络原有拓朴结构
缺点	增加额外设备(集线器) 流量大时，对网络传输性能影响大，不适合在大型网络	需要占用一个交换端口 流量大时，可能对网络传输性能有一定影响	成本较高 需要额外设备(分接器) 需要双网卡支持 安装的机器不能上网
总结	集线器是共享工作模式，是早期连接网络的主要设备，现在已经被性能更高的简易交换机代替。集线器适合在小型网络使用。	管理型交换机以及一些三层路由具备端口镜像功能，此功能可让管理人员在交换网络上进行管理。端口镜像可以一对多或一对一进行镜像，使用灵活，是较为广泛的管理方式。	分接器可以非常灵活的部署在网络的任意一个链路，在对网络性能要求非常高时，可采用 TAP 串接网络进行产品部署，不过成本高，对此方法的使用有一定的影响。

注意: 不同的交换机或不同的型号，镜像配置方法的有些区别，我们在网站上为用户提供了常见交换机的端口镜像配置方法。

四．安装与卸载

在安装产品时，请仔细阅读系统要求和 ReadMe.txt 文件；在安装之前，请先卸载以前的版本。

1. 产品安装:

请在安装之前关闭其它所有正在运行的程序，安装文件为.exe 的执行文件，双击此文件开始进入产品安装向导。
请仔细阅读使用许可协议，您必须接收该协议才能继续安装，点下一步继续。
请指定程序的安装路径，点一点步继续。
安装程序将在开始菜单中创建快捷方式，点下一步继续。

选择是否创建桌面图标和快速启动图标，点下一步继续。
安装向导已经创建好安装配置，请检查一下是否正确，确定无误，点“安装”按钮，程序将自动安装到您的电脑中。
程序安装后，将提供 Readme.txt 文档，和是否启动科来网络分析系统。

2. 产品卸载：

选择产品卸载执行程序，根据卸载向导提示完成产品卸载，并重启电脑。
或者：
打开 Windows 控制面板；
选择“添加/删除程序”；
在列表中选择“科来网络分析系统”，双击或选择删除按钮。

3. 系统要求

我们建议您将科来网络分析系统 6.4 安装在 Windows 2000/XP/2003 操作平台上，因为这些操作系统更为稳定。使用此产品对电脑要求并不高，我们提供了最低的系统要求，如果您的网络比较大，需要分析的网络流量较多时，可以采用我们推荐的配置来安装我们的产品。

1. 最低配置:

P4 1.2G CPU
512 MB RAM
Internet Explorer 5.5 or higher

2. 推荐配置:

P4 3.0G CPU
1 GB RAM or more
Internet Explorer 6.0 or higher

3. 支持的操作系统:

Windows 2000 (SP 4 or later)
Windows XP (SP 1 or later) and AMD 64bit Edition
Windows Server 2003 and AMD 64bit Edition
Windows Vista

注意:

在安装科来网络分析系统 6.4 时，必须以 Administrator 的权限或 Administrators 组的权限进行安装。

4. 产品授权

在您安装完本系统正试版并第一次运行时，会弹出一个对话框要求您输入产品序列号和产品授权号。请根据授权文件正确输入授权密匙并点击“确定”，您的授权信息将被保存，此对话框将不再出现。

授权文件通常以电子邮件形式发送给您，里面包含您运行和使用本系统所需的所有信息。请妥善保存授权文件以备后用。 如果您购买的是有外包装的产品，授权号帖在《用户使用手册》中，您需要刮开保护层，方能看到产品授权号。产品序列号在产品外包装或用户信息卡上可以看到。

授权信息
请输入正确的产品授权信息.
用户名: Nicholas
公司: 成都科来软件有限公司
序列号:
授权号:
确定 取消 帮助(H)

与授权文件、序列号和授权号有关的所有条款和条件受使用许可协议的约束。

5. 产品激活

产品激活是防止盗版的一种措施，是保护合法用户使用权益的有效手段。一个产品授权只能绑定在一台服务器（或 PC 上），产品激活一定后，即使产品重装，也不用再激活。但操作系统重装，需要重新激活产品。科来网络分析系统 6.4 提供两种激活方式：

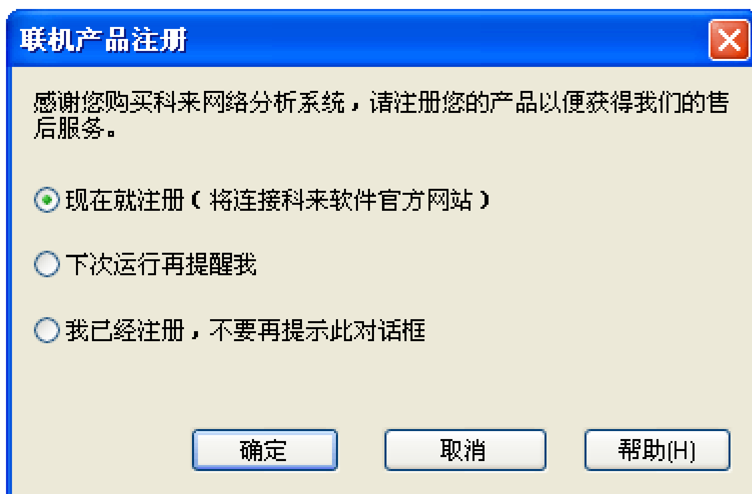
在线激活：
这是最简单的方式，只要点击在线激活，系统将自己连接到产品服务器进行授权验证。此过程只需要短短几秒钟时间就可以完成，但需要安装的机器能连上互联网。

手动激活：
此方式是为安装机器不能连上互联网时提供的操作方式。用户可将"产品序列号"和"产品安装号"通过邮件或传真方式发送给我们，我们收到用户的信息后，会向用户返回产品激活号，将激活号输入到指定地方，即可完成产品激活。

如果激活产品，最多允许用户使用 15 次，超过 15 次，就必须激活产品才能使用。

6. 产品注册

在您安装完本系统正试版并第一次运行时，会弹出一个对话框协助您对产品进行注册，以便获得科来软件的售后服务。



选择"现在就注册"，本系统将登录到科来软件官方网站进行在线注册；选择"下次运行再提醒我"，本系统将跳过注册提示；如果选择"我已经注册，不要再提示此对话框"，本系统以后不会再提示用户进行产品注册。

您也可直接登录此链接进行产品注册：
https://secure.colasoft.com/customer/main.php?module=customer_cp&action=register.

五．快速使用

在完成产品安装注册后，我们需要了解一下的产品相关的基本操作，包括启动方式、数据捕获、显示选项、数据排序，数据保存等。

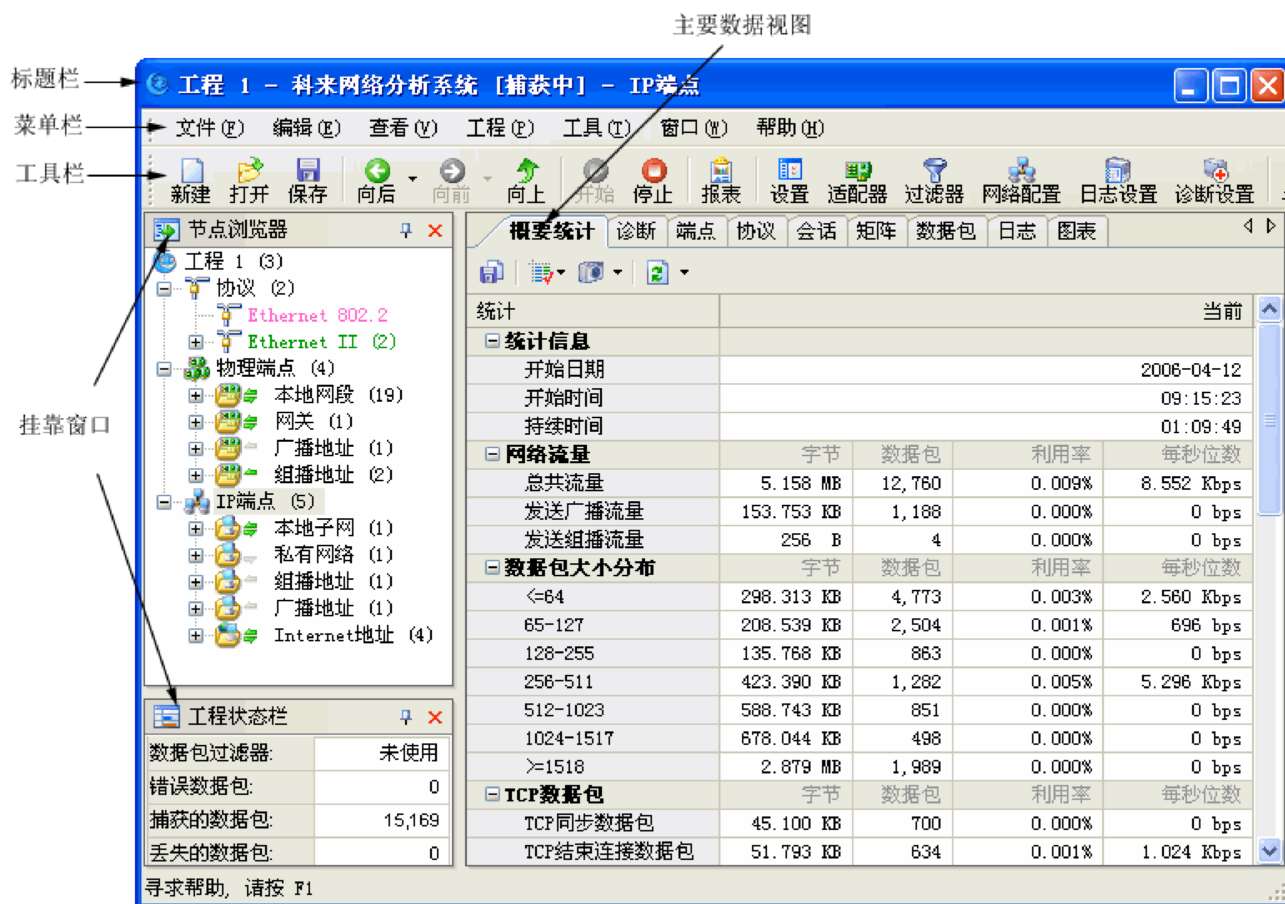
这一章还涉及到后面几章要介绍的内容，包括：

工程概念

主要数据视图

工程设置

系统选项



1. 启动方式

当完成产品安装后，将在“桌面”和“开始菜单”建立系统的快捷方式中。您可以通过以下方法来启动科来网络分析系统 6.4。

使用桌面图标
如果选择了在桌面建立快捷方式，你可以在操作系统的桌面上，双击科来网络分析系统 6.4 图标来启动程序。

使用快速启动栏
快速启动栏的科来网络分析系统图标来启动程序。

使用开始菜单
打开开始菜单，选择所有程序，点击科来网络分析系统 6.4 启动程序。

通过命令行
通过命令行 Capsa50u.exe [/command1 <file>] 来启动科来网络分析系统，详细内容请查看 “命令行支持”。

2. 捕获数据包

要进行网络分析，我们必须要对网络中的数据包进行捕获，通过对捕获到的数据包进行统计分析，才能了解当前的网络状况。

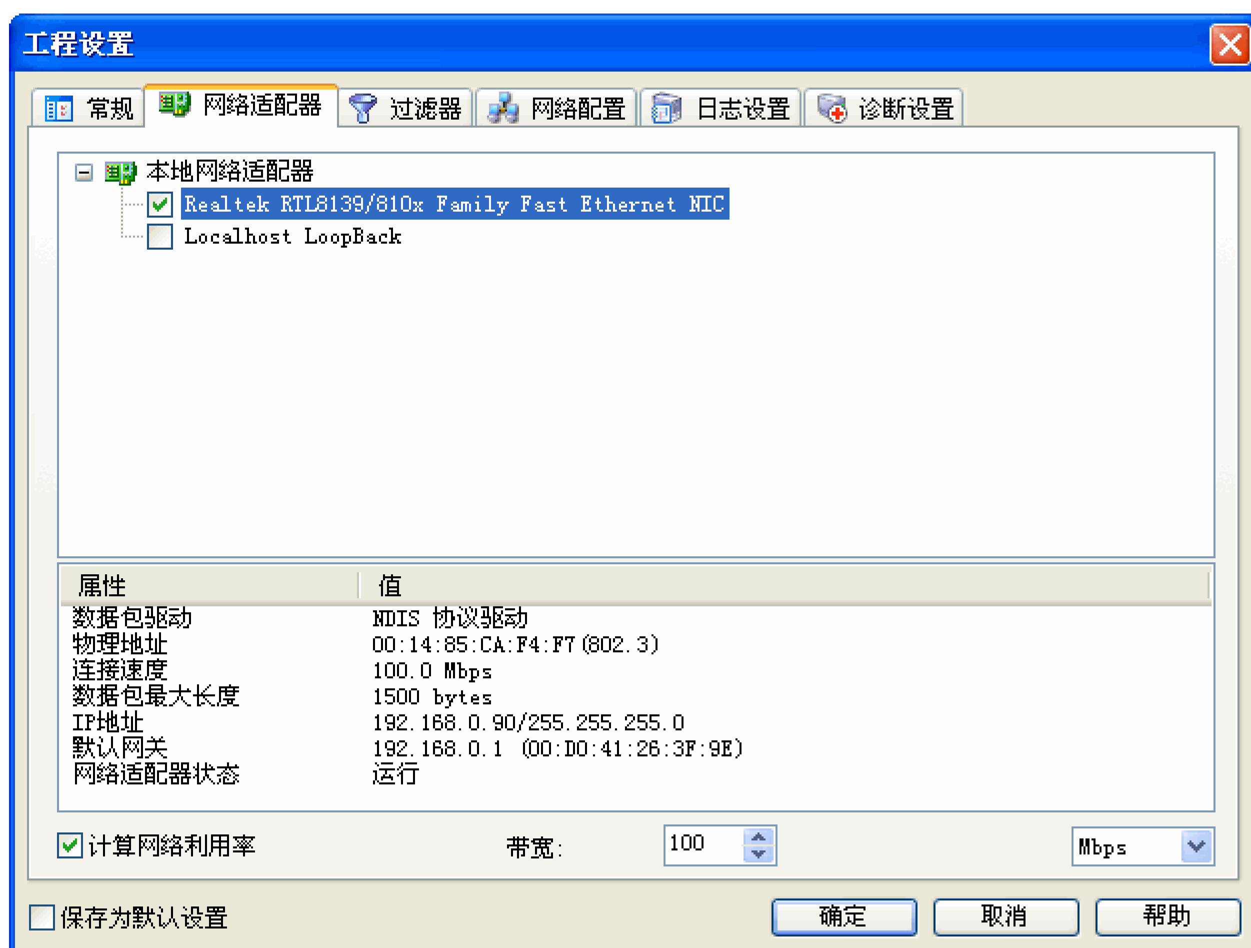
通常，您可以选择“工程”菜单中的“开始捕捉”和“停止捕捉”命令来激活科来网络分析系统或使其处于静止状态，也可以随时点击工具栏中的“开始”和“停止”图标来控制工程的状态。

3. 选择网卡

网络数据包是通过网卡进行转发的，对数据包的捕获需要利用网卡进行采集，在进行工程运行之前，需要选择分析的网卡。

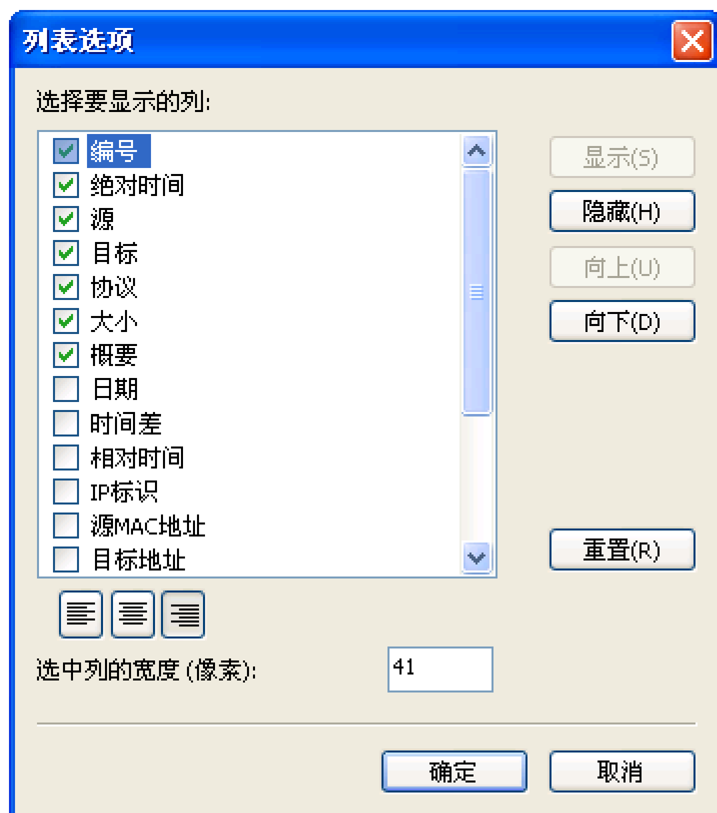
科来网络分析系统 6.4 支持多网卡进行数据采集，同时也支持拨号的上网和本地环回。本地环回是指客户端和访问的服务器端都是本机，此时的网络数据并不经过网卡，科来网络分析系统 6.4 同样支持以类数据的监测分析。

在工程设置中，科来网络分析系统会自动列出所有可用到的网卡类型，用户可以根据实际情况进行选择。



4. 设置显示选项

科来网络分析系统 6.4 的每一个视图都为用户提供了非常丰富的统计字段，为了适合查看，并没有所有的字段都显示出来。用户可以通过列表选项来设置显示的数据，右键点击每个视图字段标题，将可以打开显示选项。



5. 数据排序

数据排序功能是一个对数据查看很有用的功能，用户对于想查看的数据排序，只需要单击一下列表的字段，就可以进行正序或倒序的排列，如下图所示。

查找带宽占用最大的 IP，或查找数据包发送最多的 IP，利用数据排序将是非常容易的方法。

All
Physical
IP

可选择不同的端点类型　　按“总流量”排序，也可按其它列排序

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

类型 IP　　端点: 43

名称	总流量	数据包	每秒位	网络连接
192.168.0.90	2.150 MB	4,657	0 bps	111
192.168.0.208	2.056 MB	4,262	0 bps	102
www.colasoft.com.cn	59.135 KB	135	0 bps	2
207.46.114.54	27.211 KB	181	0 bps	1
192.168.0.255	25.324 KB	195	0 bps	0
192.168.0.211	6.264 KB	65	0 bps	0
207.46.26.50	4.723 KB	44	0 bps	2
192.168.0.28	3.796 KB	33	0 bps	0
rad.msn.com.nsatc.net	1.784 KB	11	0 bps	2
192.168.0.129	1.729 KB	13	0 bps	0
www-china.l.google.com	1.318 KB	10	0 bps	1
tools.l.google.com	1.249 KB	9	0 bps	1
192.168.0.45	1.153 KB	9	0 bps	0
192.168.0.62	1.152 KB	11	0 bps	0
192.168.0.29	1.112 KB	9	0 bps	0
192.168.0.10	1.112 KB	9	0 bps	0
192.168.0.210	1.060 KB	8	0 bps	0
192.168.0.206	657 B	5	0 bps	0
61.139.2.69	636 B	6	0 bps	0
192.168.0.207	458 B	3	0 bps	0
192.168.0.92	348 B	2	0 bps	0
192.168.0.60	343 B	2	0 bps	0
192.168.0.123	343 B	2	0 bps	0

6. 数据复制

选择数据范围，点击右键，就可选择复制方式。科来网络分析系统 6.4 提供多种数据复制方式，如下所示：

命令	描述
复制	以文本方式复制选择的内容。
复制树结构	复制鼠标所在的树的所有数据。
复制 Hex	复制数据包解码中 Hex 格式内容。
复制文本	复制数据包解码的文本内容。
复制数据列	复制指定的数据列（字段内容）。

复制的内容可以粘贴到 Excel、Word 以及其它的文本编辑器中。

7. 导入导出

导入

科来网络分析系统 6.4 支持多种通用数据包格式的导入，你可以导入数据包文件到工程中进行分析。支持的文件类型包括：



*.cscpkt (科来网络分析系统 5.5 数据包文件)

*.cpf (科来网络分析系统 4.0 数据包文件)

*.cap (Network Associates Sniffer 数据包文件)

*.pkt (EtherPeek/TokenPeek/AiroPeek 数据包文件)

*.pkt (Etherpeek Packet File V7)

*.pkt (Omnipeek Packet File V9)

*.rawpkt (Raw 数据包文件)

*.cap (Libpcap Tcpdump,Ethereal,等通用数据包文件)

*.cap (Microsoft Network Monitor 2.x)

导出

对于数据的保存，除了保存为工程文件外，你也可以将数据内容导出到一个特定格式的文件。科来网络分析系统 6.4 **除了支持基本的***.txt、*.csv、*.html **格式的文件，也支持通用的** Sniffer、Etherpeek **等工具的文件格式。 用户也可以设置需要导出的数据内容，如下图所示：**



*.txt（文本文件）

*.csv（csv 文件）

*.html（html 文件）

*.cscpkt（科来网络分析系统 5.5 数据包文件）

*.cap（Sniffer 数据包文件）

*.pkt（EtherPeek/AiroPeek 数据包文件）

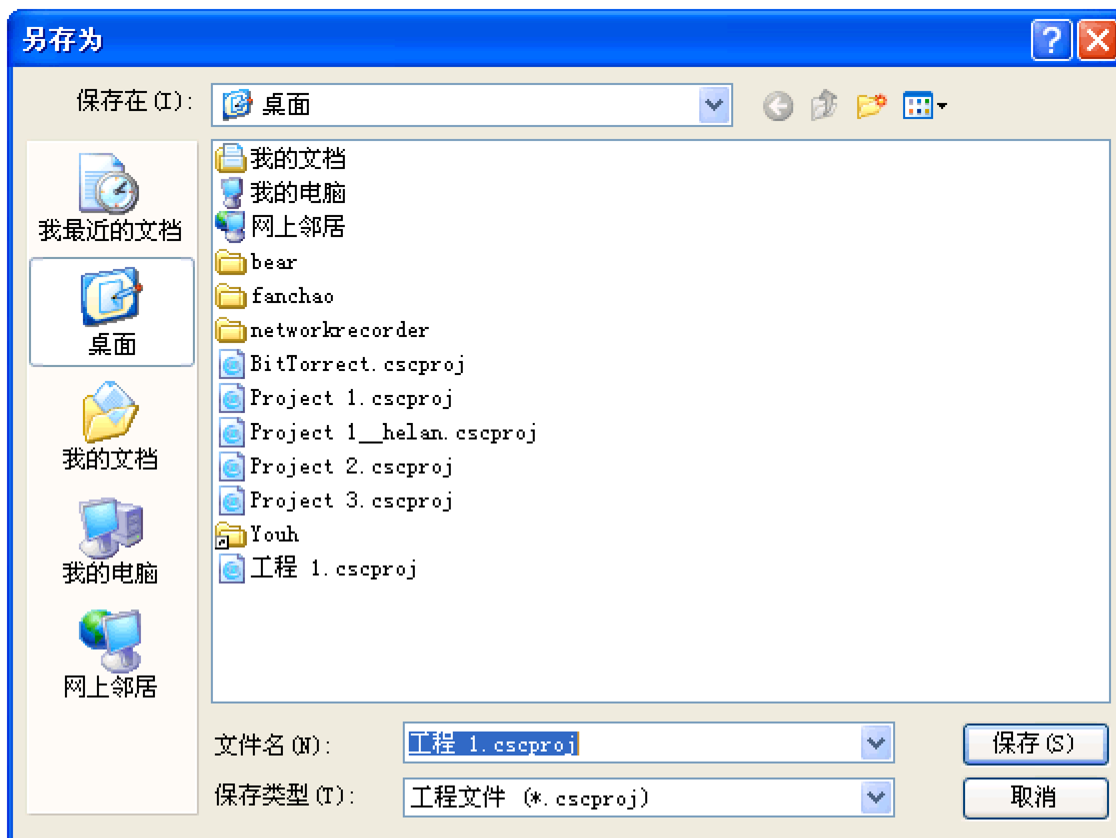
*.rawpkt（Raw 数据包文件）

*.cap（Libpcap Tcpdump,Ethereal,等通用数据包文件）

*.cap（Microsoft Network Monitor 2.x）

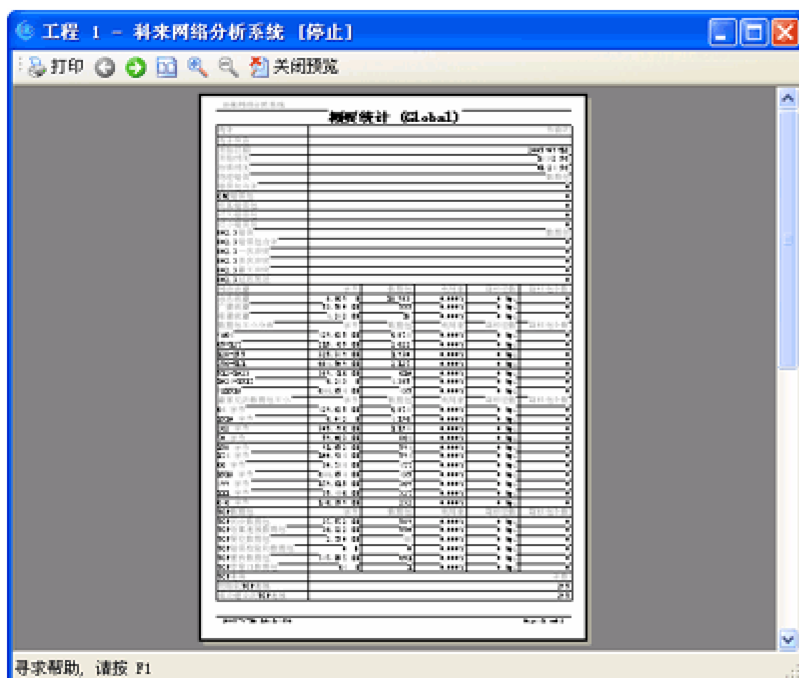
8. 工程保存

工程保存有利于以后对数据进行再次查看。您可以通过保存工程文件来保存当前的分析结果，同时也能保存工程设置中的所有选项。



9. 打印

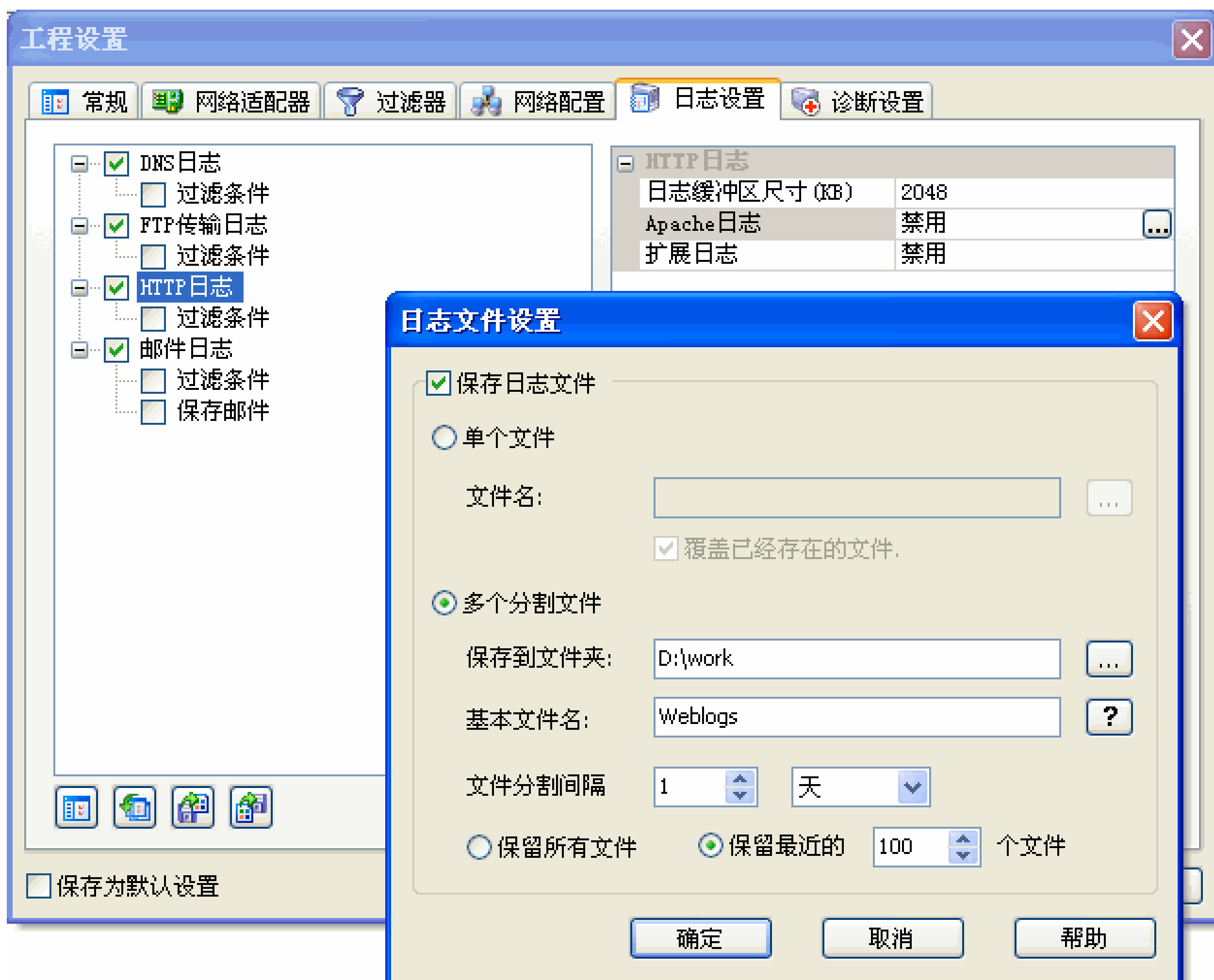
在停止状态下，可以对选择的数据进行打印。你只需要打开相应的视力，点击文件菜单中的打印图标
或 Ctrl + P，则可进行打印了。
在打印这前，建议对打印的数据进行打印预览，打印预览可以向用户展示打印的效果。



10.生成日志

科来网络分析系统 6.4 提供的高级分析模块，都提供日志功能，您可以将高级分析模块的结果以日志方式保存。

点击工具栏图标 即可对生成的日志进行配置，您可选择是否保存每个分析模块的日志，并且可自定义日志保存的位置。日志文件可以按照日期或文件大小来分割成单独的文件，同时也可定义日志保存的数量，使日志文件不会无限增加。



六．工程

工程可以被理解为一次分析任务。工程文件包含网络分析的配置和统计分析数据，保存了工程文件也就保存了当前的分析设置和分析结果，用户可以日后查看当前的网络状况。

工程都有一个默认设置，用户可以通过“工程设置”来调整网络分析的范围和用途，如果不改变设置，只需要点运行，即可开始进行数据采集和分析。

当有数据被捕获后，用户会看到下图所示界面，我们简单介绍一下：

窗口标题栏

窗口标题栏中显示软件的名称、版本号和当前工程的名称。

菜单栏

包括“文件”菜单、“编辑”菜单、“视图”菜单、“工程”菜单、“工具”菜单、“窗口”菜单和“帮助”菜单，分别提供不同的菜单命令。

工具栏

当工具栏被启用时（默认模式），包括多个代表特定菜单命令的快捷按钮。要显示或隐藏工具栏，可在“视图”菜单中选中或取消选中“工具栏”一项。

开始页

开始页是在创建新工程时出现，为用户提供相关信息和选择，用户可以打开最近使用过的工程，也可通过模板创建工程。

挂靠窗口

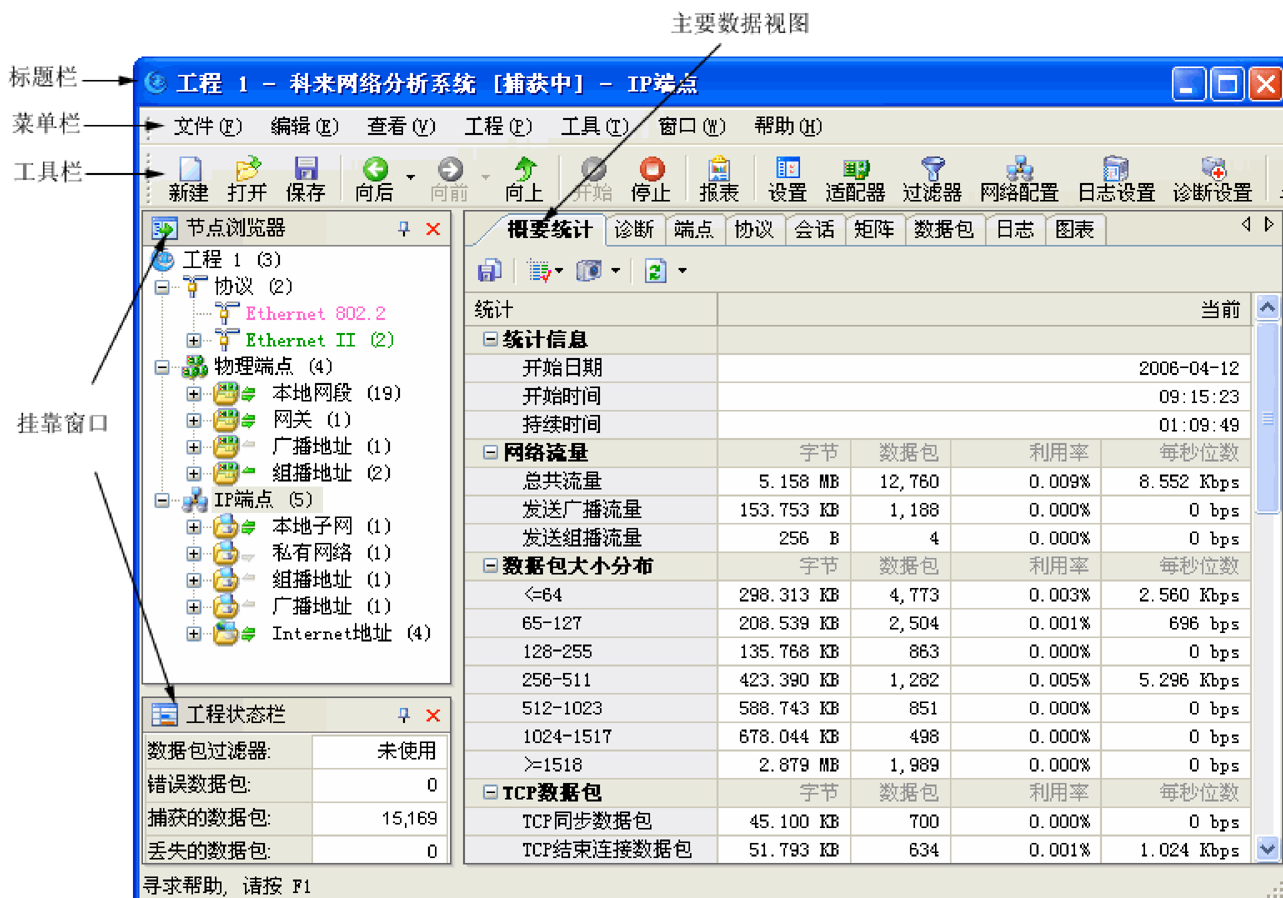
可以任意挂靠的窗口，我们称为挂靠窗口，用户可以拖动窗口栏来改变这些窗口的位置。“节点浏览器”和“工程状态栏”就属于挂靠窗口。

“节点浏览器”最大的用途，就是能快速的选择需要查看的节点，通过选择节点，用户可以查看该节点对应的网络数据。

“工程状态栏”提供当前工程的执行情况和设置状态。包括使用的过滤器，捕获到的数据包，数据包缓存的占用情况等。

主视图区

主视图区在窗口的右边，包括概要统计视图、端点视图、协议视图、数据包解码视图、会话视图、矩阵视图、日志视图、图表视图。点击相应的视图标签，则可以查看相应的网络分析数据。



1. 菜单

下面的表格是菜单命令以及相应说明：

命令	快捷键	描述
		文件
新建	Ctrl+N	创建一个新的工程
选择模板新建...		利用现有的模板创建工程
打开...	Ctrl+O	打开一个存在的工程文件
保存	Ctrl+S	保存工程文件
另存为...		将工程文件另存为一个新的文件
另存为模板...		将当前的工程设置另存为模板
关闭		关闭当前的工程
打印...	Ctrl+P	打印当前的工程视图数据
打印预览		预览打印效果
打印设置...		设置打印时的选项
导入...		将数据包文件导入到当前工程文件中
导出...		将当前的工程数据导出为一个数据包文件
最近打开的工程文件		显示最近使用的工程文件，用户可以快速的打开这些历史文件
退出		退出程序
		编辑
剪切	Ctrl+X	将所选内容剪切到剪贴板
复制	Ctrl+C	将所选内容拷贝到剪贴板
粘贴	Ctrl+V	粘贴将复制的内容
删除	Del	删除选择内容
查找...	Ctrl+F	查找
查找前一个	Shift+F3	查找前一个结果
查找下一个	F3	查找下一个结果
全选	Ctrl+A	选择全部内容
		查看
工具栏		放置功能快捷图标
状态栏		显示当前窗口或视图的状态
跳至		改变当前窗口到历史窗口
节点浏览器		节点浏览器
工程状态栏		提供当前工程的执行情况和设置状态。包括使用的过滤器，捕获到的数据包，数据包缓存的占用情况等。
技术论坛		进入相关论坛
显示网卡厂商		将 MAC 地址有前六位数字显示为网卡厂商的名称
显示主机名		解析 IP 的主机名，并显示
显示端口名		将端口号显示为标准的端口名称
刷新	F5	刷新当前视图或数据
		工程
开始捕获	F2	开始捕获网络数据包
停止捕获		停止捕获网络数据包
清空数据包缓存...		丢弃当前工程数据包缓存中的所有数据包
清空工程...		清空当前工程中除工程设置以外的所有数据
生成报表...		将当前的分析结果生成一个 HTML 格式的报表文件

设置...	设置工程选项，设置结果将立即生效
网卡...	选择进行数据包捕获的网卡
过滤器...	打开过滤器设置对话框
网络配置...	打开网络配置设置对话框
日志设置	打开高级日志设置对话框
诊断设置	打开网络自动诊断设置对话框
工具	
名字表	打开名字表对话框
过滤器表	打开过滤器表对话框
数据包采集驱动...	打开数据包采集驱动对话框，你可安装改变采集数据包的驱动程序
选项...	打开系统选项对话框
窗口	
新建窗口	打开一个新的窗口来显示同一工程内容，方便于数据对比。
关闭	关闭当前窗口
下一窗口	切换到下一个窗口
前一窗口	切换到上一个窗口
帮助	
帮助主题	打开产品帮助，并切换到帮助主题。
帮助查找...	打开产品帮助的搜索
帮助索引	打开产品帮助的索引
技术支持	打开产品帮助的技术支持内容
产品激活...	打开产品激活向导
检查最新版本	检查是否有最新版本
科来软件网站	访问公司网站
关于科来网络分析系统...	访问产品的网站内容

2. 工具栏

工具栏是由图标和注释文字组成，工具栏没有完全显示所有的工具，用户也可以在工具栏上点鼠标右键进行自定义。



3. 开始页面

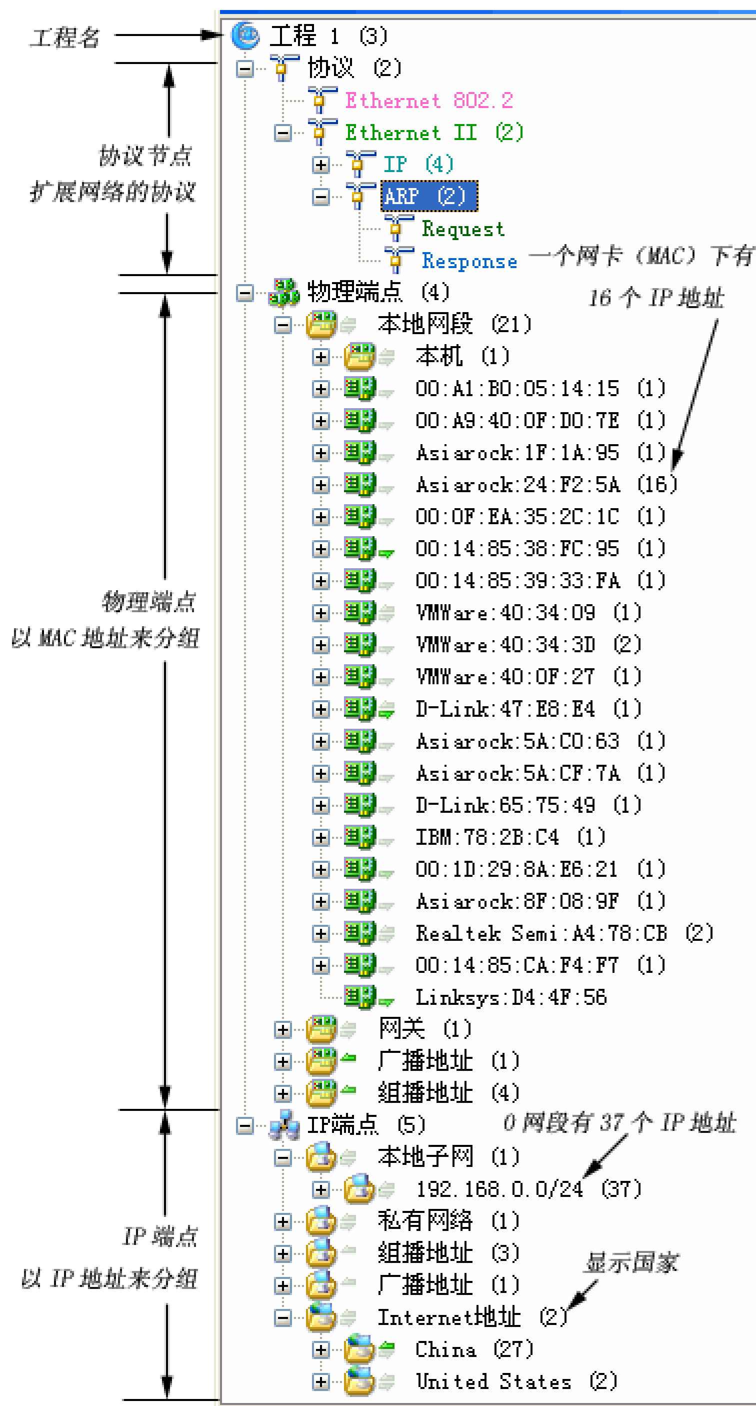
开始页是在创建新工程时出现，为用户提供相关信息和选择，用户可以打开最近使用过的工程，也可通过模板创建工程。

如果用户不需要更改默认的配置，点击“立即开始采集”按钮，就可快速开始对网络进行分析了。



4. 节点浏览器

节点浏览器最大的用途，就是能快速的选择需要查看的节点，通过选择节点，用户可以查看该节点对应的网络数据。节点浏览器由三个类组成，分别是协议节点，物理节点，IP 节点。用户可以很方便的定位到整个网络，也可以定位到某个 IP 段，或是某个 IP。而右边的数据会根据选择的节点显示相关的数据。



5. 工程状态栏

我们为每个工程都提供一个状态栏，用户可以查看当前工程的执行情况和配置状态。包括使用的过滤器，捕获到的数据包，数据包缓存的占用情况等。

缓存使用率的颜色条默认情况下是蓝色，超过 80%，将变为橙色，超过 90%，则显示为红色。

工程状态栏	
数据包过滤器:	未使用
错误数据包:	0
捕获的数据包:	908,280
丢失的数据包:	0
接受的数据包:	908,280
拒绝的数据包:	0
缓存使用率:	16,383 KB

七．主视图区

网络分析的主要数据结果，都放置在主视图区。科来网络分析系统 6.4 包含以下视图，每个视图都包含不同的分析结果。

视图	视图功能描述
概要统计	提供近百个统计计数器为用户提供非常详尽的网络统计信息，快照功能允许用户对特定时段的数据变化进行比较。
诊断	网络内的错误信息或故障信息，进行自动提示，用户可以不必去了解数据包的详细内容，便可以从专家诊断模块中获得网络内的错误和故障分析。
端点	端点分为物理端点和 IP 端点，通过网络端点统计分析功能，用户可以快速找定位通讯量最大的 IP 端点和物理端点。
协议	遵循 OSI 七层协议，根据实际的网络协议封装顺序，层次化得展现给用户，每个协议有自己的色彩，除了全局的协议统计，还可提供每个网络端点下的协议统计数据。
会话	提供物理地址、IP 地址、TCP 连接、UDP 会话的通讯情况，通过查看会话，可以统计出其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。
矩阵	矩阵视图可对网络中通讯的节点和会话进行详细统计，通过统计我们可了解到整个网络通讯的节点/会话信息、某台物理主机/IP 主机的通讯节点/会话信息、以及某条会话的主机信息；
数据包	数据包解码是实时完成的，分别向用户提供概要解码、字段解码、十六进制解码。通过查看数据包内容，我们可以对网络问题进行精确定位，可以清楚地了解应用的来源和其他细节，从而在庞杂的数据流中找出那些可能存在的问题。
日志	支持 DNS、HTTP，Email 以及 FTP 日志分析，除了即时查看外，还可以生成日志文件，日志文件可以按时间或文件大小 进行自动分割。
图表	为用户提供 2D 或者 3D 的时间趋势图和数据比较图，可以选择折线图、柱状图、面积图、饼图等多种形式，除了全局图表，也支持每个协议和网络端点的图表数据采集显示。

每个视图都有自己的工具栏，用户可利用这些视图工具对数据进行过滤、筛选、复制等操作。

在对分析结果进行查看时，我们可以利用数据排序来进行数据快速筛选。要分离出带宽占用最大或网络最活跃的主机，是件非常容易的事。

All
Physical
IP

可选择不同的端点类型　　按“总流量”排序，也可按其它列排序

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表

类型 IP　　端点：43

名称	总流量	数据包	每秒位	网络连接
192.168.0.90	2.150 MB	4,657	0 bps	111
192.168.0.208	2.056 MB	4,262	0 bps	102
www.colasoft.com.cn	59.135 KB	135	0 bps	2
207.46.114.54	27.211 KB	181	0 bps	1
192.168.0.255	25.324 KB	195	0 bps	0
192.168.0.211	6.264 KB	65	0 bps	0
207.46.26.50	4.723 KB	44	0 bps	2
192.168.0.28	3.796 KB	33	0 bps	0
rad.msn.com.nsatc.net	1.784 KB	11	0 bps	2
192.168.0.129	1.729 KB	13	0 bps	0
www-china.l.google.com	1.318 KB	10	0 bps	1
tools.l.google.com	1.249 KB	9	0 bps	1
192.168.0.45	1.153 KB	9	0 bps	0
192.168.0.62	1.152 KB	11	0 bps	0
192.168.0.29	1.112 KB	9	0 bps	0
192.168.0.10	1.112 KB	9	0 bps	0
192.168.0.210	1.060 KB	8	0 bps	0
192.168.0.206	657 B	5	0 bps	0
61.139.2.69	636 B	6	0 bps	0
192.168.0.207	458 B	3	0 bps	0
192.168.0.92	348 B	2	0 bps	0
192.168.0.60	343 B	2	0 bps	0
192.168.0.123	343 B	2	0 bps	0

对于视图中显示的内容，用户也可以根据自己的需要，对数据显示进行设定。

科来网络分析系统 6.4 的每一个视图都为用户提供了非常丰富的统计字段，为了适合查看，并没有所有的字段都显示出来。用户可以通过列表选项来设置显示的数据，右键点击每个视图字段标题，将可以打

开显示选项。

列标题（统计字段）

在列标题栏点击右键，确定需要显示的项打勾的会在视图中显示



1. 概要统计

科来网络分析系统的统计功能非常强大，近百个统计计数器为用户提供非常详尽的统计信息，快照功能允许用户对特定时段的数据变化进行比较。概要统计不仅是全局的，每个网络协议和网络端点都有自己的概要统计，用户可以开启多个窗口，比较不同协议或端点之间的概要统计。

另存为 显示选项 快照 刷新

概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表

统计					当前
⊟ 统计信息					
开始日期					2006-04-12
开始时间					09:29:00
持续时间					00:10:30
⊟ 物理错误					数据包
错误包合计					0
CRC错误包					0
对齐错误包					0
过大错误包					0
过小错误包					0
⊟ 802.3错误					数据包
802.3错误包合计					0
802.3一次冲突					0
802.3多次冲突					0
802.3最大冲突					0
802.3延迟发送					0
⊟ 网络流量	字节	数据包	利用率	每秒位数	每秒包个数
总共流量	2.197 MB	5,216	0.001%	512 bps	1
发送广播流量	28.436 KB	243	0.000%	0 bps	0
发送组播流量	256 B	4	0.000%	0 bps	0
⊟ 数据包大小分布	字节	数据包	利用率	每秒位数	每秒包个数
<=64	122.125 KB	1,954	0.001%	512 bps	1
65-127	45.733 KB	556	0.000%	0 bps	0

"-"，展开统计信息
"+"，收缩统计信息

以下是概要统计中统计信息介绍：

名称	描述
统计信息	显示科来网络分析系统开始运行的日期、时间，以及持续运行的时间。
物理错误	显示网络中的物理错误数据包数，包括 CRC 错误、对齐错误、过大数据包错误和过小数据包错误。如果系统捕获到网络中有较多此类物理错误的数据包，表示当前网络的物理层可能存在故障，具体可能是由网络设备及线路干扰过大、网线 RJ45 头损坏、接触不良、线路两端设备速率不匹配等情况造成。
802.3 错误	显示网络中 IEEE802.3 错误的数据包数，包括 802.3 一次冲突错误、802.3 多次冲突错误、802.3 最大冲突错误和 802.3 延迟发送错误。当网络中出现较多此类物理数据包时，表示网络的传输存在故障，具体可能是由网络阻塞、两端设备速率模式不匹配、传输线路超出规定范围、网络设备（如网卡）硬件错误等情况造成。
网络流量	显示网络中数据通讯的流量占用情况，包括总共流量、广播流量和组播流量。对每种流量，又可详细统计出其字节，数据包，每秒数据包，利用率等信息，通过这些信息，我们可以知道当前网络的总体工作状态，当总共流量的利用率超过 50%，表示网络的负载过重；广播流量或组播流量大于总流量的 20%，表示网络中可能存在广播/组播风暴或 ARP 攻击。
数据包大小分布	显示网络中数据包的大小分布情况，不同大小的数据包，都可对其总共字节、数据包数、每秒数据包数、以及利用率等信息进行统计，通过数据包大小分布，可以知道网络的通讯质量，如当<=64 或>=1518 的数据包过多，占用总流量比例过大时，表示网络中可能存在非正常的网络通讯，如碎片或数据包溢出攻击。
最常见的	显示网络中数量最多的数据包的大小以及这些数据包的流量占用情况，包括这些数据包的个

数据包大小	数，占用字节数，每秒数据包数以及利用率等信息。通过这些信息，我们可以知道当前网络通讯中最多的数据包是什么，并判定其相应的服务，如 1518 和 64 字节左右的数据包排在前两位，表示网络中可能存在大文件的上传下载操作；另外，如网络中某固定大小的数据包占用流量及利用率均很高，表示网络中可能存在 DOS/DDOS/DRDOS 攻击。
TCP 数据包	显示网络中的 TCP 数据包数，包括 TCP 同步数据包、TCP 结束连接数据包、TCP 复位数据包、TCP 错误检验和数据包、TCP 重传数据包以及 TCP 零窗口数据包，对每一种 TCP 数据包，都可以显示出其占用字节数，数据包个数，每秒数据包数以及利用率等信息，通过这些信息，可以知道网络中的通讯是否正常。如 TCP 同步数据包和 TCP 复位数据包大大超过其他类型数据包时，表示网络中可能有扫描器在工作，或者网络中有主机正在被扫描攻击；当 TCP 重传数据包过多时，则表示网络的通讯质量极低，可能存在环路现象；当 TCP 零窗口数据包较多时，表示对端主机当前无法接受数据，对方主机系统可能存在故障。
TCP 连接	显示网络中的 TCP 连接数，可统计出初始化的 TCP 连接数、成功建立的 TCP 连接数、拒绝的 TCP 连接数和复位的 TCP 连接数。通过对这些信息的统计，我们可以知道网络中的 TCP 通信是否正常，如初始化的 TCP 连接数较多，而成功建立的 TCP 连接数很少时，表示网络中的主机可能感染病毒，且此病毒正在试图连接其他主机的某些 TCP 端口以进行感染；拒绝的 TCP 连接数较多时，表示网络可可能存在端口扫描攻击或用户名密码破解攻击。
SMTP 分析	显示使用 SMTP 协议进行邮件发送的信息，包括建立的 SMTP 连接数，失败的 SMTP 连接数、服务器应答错误数，以及发送的邮件数等等。通过这些数据，我们可以确定网络中的邮件发送是否正常，如网络中的 SMTP 服务器工作是否正常（包括工作效率）；网络中的 SMTP 服务器是否可能被黑客控制，正被用于处理垃圾邮件；网络中是否存在感染蠕虫病毒的主机；网络中是否存在破解邮箱用户名密码的情况。
POP3 分析	显示使用 POP3 协议进行邮件接收的信息，包括建立的 POP3 连接数，失败的 POP3 连接数、服务器返回错误数，以及接收的邮件数等等。通过这些数据，我们可以确定网络中的邮件接收是否正常，如邮件的 POP3 服务器是否正常工作（包括其工作效率）；网络中是否存在破解邮箱用户名密码的情况。
FTP 分析	显示网络中 FTP 传输数据包的统计信息，包括 FTP 控制连接数、登录失败次数、成功的数据连接数、以及访问的服务器数等。通过这些信息，我们可以确定网络中进行 FTP 数据上传下载的情况，包括 FTP 服务器的数据是否被未被允许的上传下载，网络中是否存在 FTP 账户的用户名密码的情况，以及对上传下载的数据进行统计。
HTTP 分析	显示网络中上网的统计信息，包括 HTTP 连接数、HTTP 请求数、通过 HTTP 端口传输非 HTTP 数据的连接数、访问过的 HTTP 服务器数等。通过这些信息，我们可以对网络中的网页浏览进行统计，并确定网络中是否存在使用 HTTP 代理的程序，如通过 HTTP 端口传输非 HTTP 数据的连接数较大时，说明网络中可能正在运行使用 HTTP 代理服务器工作的程序，如 QQ、MSN 等 P2P 软件。
DNS 分析	每条日志均表示服务器端返回的一个 DNS 响应。对于每条日志信息，可以捕获并统计出其对应客户端地址、客户端端口、服务器端地址、服务器端端口、查询的域名、请求是否成功、服务器端的回答、权威回答、附加效果、以及具体的分析结果。通过这些信息，可以有效查看网络中所有用户或特定用户的 DNS 请求及响应情况。

2．诊断

专家诊断是科来网络分析系统 6.4 的重要功能，可以将捕获到的数据进行智能化的分析，对网络内的错误信息或故障信息，进行自动提示，用户可以不必去了解数据包的详细内容，便可以从专家诊断模块中获得网络内的错误和故障分析。

诊断视图分为上下两个视图，上面的视图是按照 OSI 七层协议对错误信息进行分组，目前产品支持四个层次的故障诊断：应用层、传输层、网络层、数据链路层。用户可以分别查

看不同协议层都有哪些网络错误和故障。而网络错误和故障都有安全级别的划分，有的是普通信息提示，有的是严重的错误警告，如下表所示：

安全级别	图标	描述
消息		普通信息通知，只是用来记录某个事件，并没有网络错误。
注意		对网络事件或特定事件进行提示，需要用户引起重视的内容。
警告		对错误或故障进行警告提示，用户应该及时处理。
危急		这是对严重错误或严重故障进行提示，用户需要及时处理。

诊断视图简图如下所示：

3. 端点

网络端点是网络通讯中的重要组成部分，是网络通讯的两端，科来网络分析系统将分为物理端点和 IP 端点，通过网络端点统计分析功能，用户可以快速找定位通讯量最大的 IP 端点和物理端点。系统还支持每个网络协议的端点流量明晰统计排名，比如用户可以知道 HTTP 协议下前 5 个 IP 端点。

另存为　端点类型　树型显示　显示细节　生成过滤器　添加到名字表　自定义列　刷新　定位节点浏览器

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

类型 IP　　端点: 43

名称	总流量	数据包	每秒位	网络连接
192.168.0.90	2.150 MB	4,657	0 bps	111
192.168.0.208	2.056 MB	4,262	0 bps	102
www.colasoft.com.cn	59.135 KB	135	0 bps	2
207.46.114.54	27.211 KB	181	0 bps	1
192.168.0.255	25.324 KB	195	0 bps	0
192.168.0.211	6.264 KB	65	0 bps	0
207.46.26.50	4.723 KB	44	0 bps	2
192.168.0.28	3.796 KB	33	0 bps	0
rad.msn.com.nsatc.net	1.784 KB	11	0 bps	2
192.168.0.129	1.729 KB	13	0 bps	0
www-china.l.google.com	1.318 KB	10	0 bps	1
tools.l.google.com	1.249 KB	9	0 bps	1
192.168.0.45	1.153 KB	9	0 bps	0
192.168.0.62	1.152 KB	11	0 bps	0
192.168.0.29	1.112 KB	9	0 bps	0
192.168.0.10	1.112 KB	9	0 bps	0
192.168.0.210	1.060 KB	8	0 bps	0
192.168.0.206	657 B	5	0 bps	0
61.139.2.69	636 B	6	0 bps	0
192.168.0.207	458 B	3	0 bps	0
192.168.0.92	348 B	2	0 bps	0
192.168.0.60	343 B	2	0 bps	0
192.168.0.123	343 B	2	0 bps	0

从上图可以清楚地得出当前网络中所有主机（包括一个网段、一个物理 MAC 地址、一个 IP）的具体流量占用情况，如总流量最大的主机、发送流量最大的主机、接收流量最大的主机、收发数据包数最多的主机、发送数据包最多的主机、接收数据包最多的主机、内部流量、以及广播流量最大的主机等信息。

通过这些信息，我们可以确定网络中是否广播/组播风暴，并帮助用户排查网络速度慢、网络时断时续、蠕虫病毒攻击、DOS 攻击、以及用户无法上网等网络故障。

4. 协议

遵循 OSI 七层协议分析，根据实际的网络协议封装顺序，层次化得展现给用户，每个协议有自己的色彩，除了全局的协议统计，还可提供每个网络端点下的协议统计数据。

另存为 显示细节 生成过滤器 自定义列 刷新

概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表 报表

定位浏览器节点

协议： 22

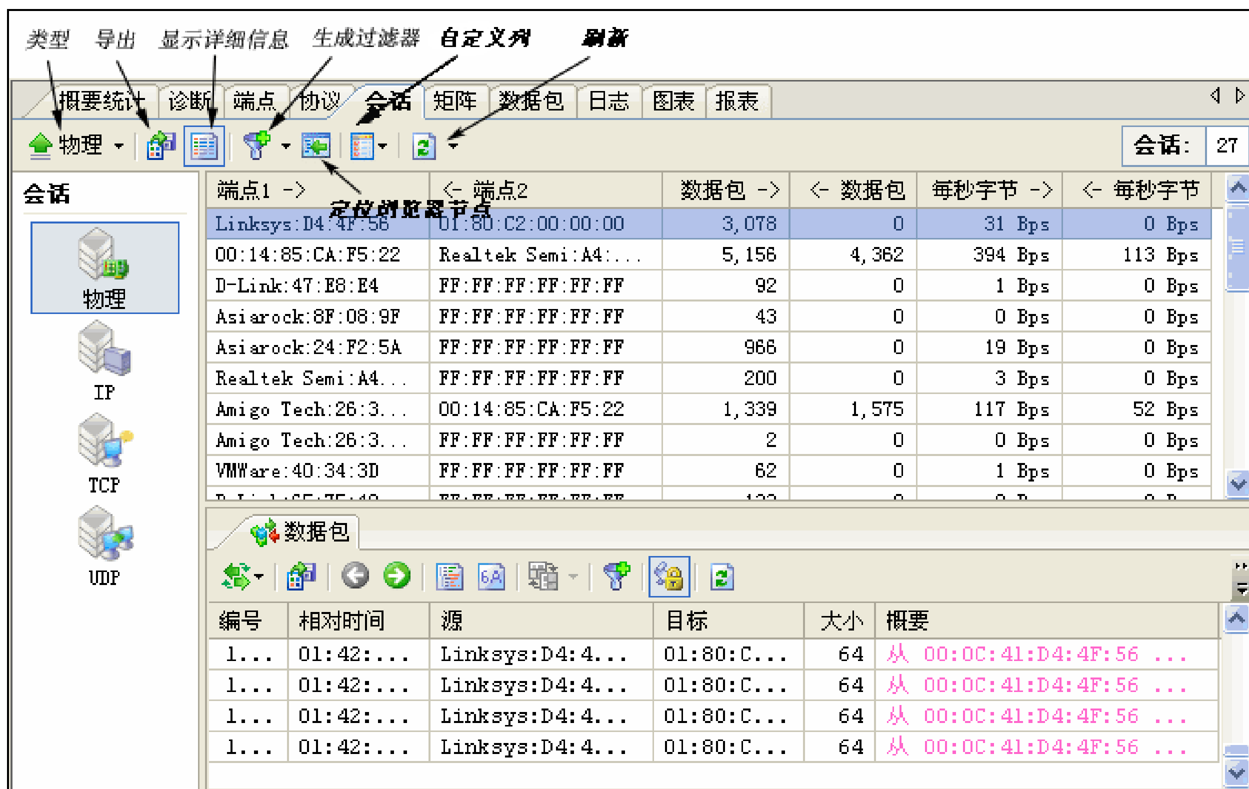
名称	流量	数据包	每秒位	网络连接
Ethernet II	2.177 MB	4,898	0 bps	111
IP	2.174 MB	4,852	0 bps	111
TCP	2.149 MB	4,647	0 bps	111
Other	1.409 MB	1,765	0 bps	3
HTTP Proxy	571.649 KB	2,058	0 bps	95
CIFS	82.107 KB	402	0 bps	1
HTTP	63.486 KB	165	0 bps	6
MSN	31.934 KB	225	0 bps	3
H.225	7.583 KB	26	0 bps	2
PPTP	390 B	6	0 bps	1
UDP	25.945 KB	201	0 bps	0
NetBIOS	25.324 KB	195	0 bps	0
Name Service	14.420 KB	151	0 bps	0
Datagram Service	10.904 KB	44	0 bps	0
DNS	636 B	6	0 bps	0
Response	393 B	3	0 bps	0
Query	243 B	3	0 bps	0
IGMP	256 B	4	0 bps	0
ARP	2.875 KB	46	0 bps	0
Request	2.813 KB	45	0 bps	0
Response	64 B	1	0 bps	0
Ethernet 802.2	19.986 KB	318	512 bps	0

协议视图可以有效显示网络中数据通讯所使用的协议，协议采用树状层级方式显示，对每一种协议，都对其占用的流量、使用此协议的数据包个数、此协议的流量在总流量中的百分比、以及使用此协议的数据包在总数据包中的百分比进行了统计，如图所示。

通过协议视图对各视图占用流量及百分比的统计，用户可以得出当前网络中占用流量最多的协议，即当前网络中占用流量最多的服务类型；并帮助用户排查网络速度慢、邮件蠕虫病毒攻击、网络时断时续以及用户无法上网等网络故障。

5. 会话

会话视图功能是科来网络分析系统 6.4 在新增的一个重要功能，通过会话视图我们可以知道当前网络的会话情况。如图所示，



会话视图提供物理地址、IP 地址、TCP 连接、UDP 会话用来显示网络中的会话信息。并在下方的子窗口中显示当前选定会话的数据包等信息。

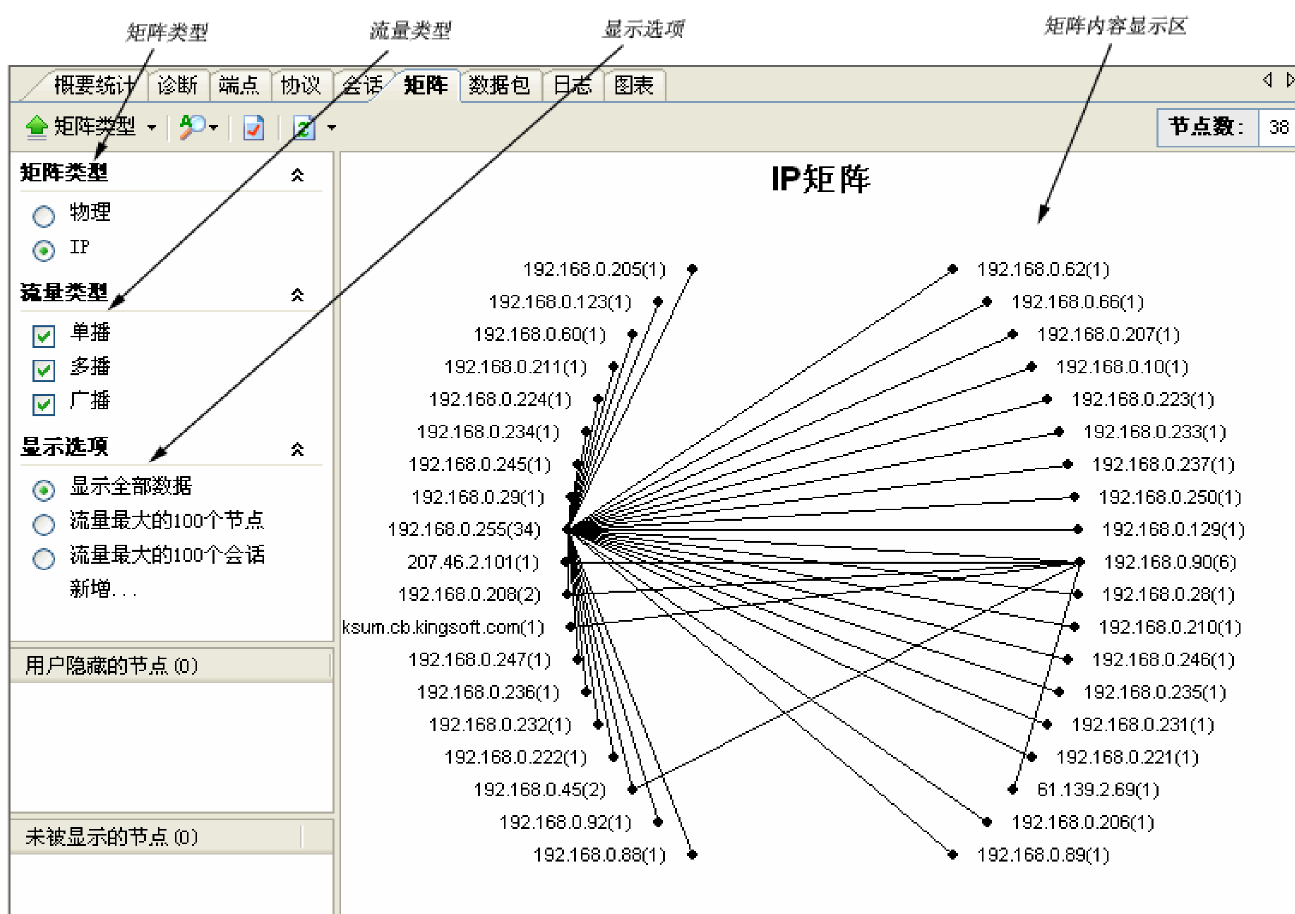
通过查看每条会话，我们可以统计其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。我们可以通过这些信息确定出当前网络中某个会话的通讯情况。

通过对会话视图的查看，管理人员可以：

- 设定显示选项，自定义要查看的数据列
- 双击打开新窗口查看会话细节
- 通过 Page UP 和 Page Down 来浏览前后连接
- 通过该会话生成过滤器
- 导出端点对数据
- 定位该会话所在节点
- 将 MAC 地址或 IP 地址添加到名字表
- 使用滚屏功能始终显示最新的会话

6. 矩阵

科来网络分析系统 6.4 新增加的矩阵视图，可对网络中通讯的节点和会话进行详细统计，其界面如下图所示。



通过矩阵视图，我们可了解到以下信息：

整个网络通讯的节点信息；

整个网络通讯的会话信息；

某台物理主机的通讯节点信息；

某台 IP 主机的通讯会话信息；

某台物理主机的通讯节点信息；

某台 IP 主机的通讯会话信息；

某条会话的主机信息；

7．数据包

数据包解码由概要解码、字段解码、十六进制解码组成，概要解码是自动进行，用户也可以选择概要解码的协议层，帮助用户快速定位可疑的网络数据包，用户还可以选择单个数据包进行详细解码，详细解码字段可以和数据包原始数据互动，即便是精心伪造的网络攻击、欺骗数据包在这种模式下也无所遁形，点击这里了解数据包解码详细信息。

概要显示视图逐行显示捕获到的数据包概要信息

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

IP\数据包: 4, 852

编号	绝对时间	源	目标	协议	大小	概要
5191	09:39:14.785363	192.168.0.90:1383	192.168.0.208:5001	TCP	64	序列号=127990287...
5192	09:39:14.785480	192.168.0.90:1382	192.168.0.208:5001	TCP	64	序列号=127969288...
5194	09:39:14.982207	192.168.0.208:5001	192.168.0.90:1382	TCP	64	序列号=065835963...
5195	09:39:14.982259	192.168.0.208:5001	192.168.0.90:1383	TCP	64	序列号=316337996...
5196	09:39:14.982270	192.168.0.208:5001	192.168.0.90:1384	TCP	64	序列号=321326757...
5197	09:39:15.024419	207.46.114.54:1863	192.168.0.90:1064	MSN	205	序列号=307526949...
5198	09:39:15.136170	192.168.0.90:1064	207.46.114.54:1863	MSN	64	序列号=102981647...
5203	09:39:20.793710	192.168.0.208:138	192.168.0.255:138	NBDGM	247	C: Transaction N...
5205	09:39:23.821893	192.168.0.90:1725	192.168.0.208:8080	HTTP Proxy	503	序列号=155568235...
5206	09:39:23.937385	192.168.0.208:8080	192.168.0.90:1725	HTTP Proxy	64	序列号=111216279...
5207	09:39:23.937457	192.168.0.90:1725	192.168.0.208:8080	HTTP Proxy	903	序列号=155568280...

数据包: 编号:005191 长度:64 捕获长度:60 时间戳:2006-04-12 09:39:14.785363
ETH II 目标:00:E0:4C:A4:78:CB 源:00:14:85:CA:F4:F7 协议:0x0800
IP 版本:4 头长:5 DSF:0000 0000 总长:46 标识:0x6DDB 标志:010. .... 段偏移:0
TCP - 传输控制协议 [34/20]
源端口: 1383 (gwha) [34/2]
目标端口: 5001 (complex-link) [36/2]
序列号: 1279902877 [38/4]
确认号: 3163379960 [42/4]

```
0000  00 E0 4C A4 78 CB 00 14 85 CA F4 F7 08 00 45 00 00 2E 6D DB 40 00 80   ..L.x.........E...m.@..
0017  06 0A 74 C0 A8 00 5A C0 A8 00 D0 05 67 13 89 4C 49 C4 9D BC 8D 58 F8   ..t...Z.....g..LI....X.
002E  50 18 FA F0 4E 52 00 00 4E 55 4C 4C 0A 0A                               P...NR..NULL..
```

(-) 表示在多行显示解码信息
(+) 表示在一行显示解码信息

字段解码视图框显示所选数据包字段的详细信息

十六进制解码

ASCII或EBCDIC解码

通过解码信息，我们可以了解以下信息：

数据包的概要信息（作用、以及提取的重要值）；

网络中的数据包的类型；

网络中传输的数据包是否正确；

网络中 IP 数据包的版本；

目标主机是否在运行客户端主机所请求的服务；

源主机到目标主机间的路由时间（即链路长度）；

目标主机对客户端主机请求的服务的响应时间；

网络中传输的数据是否为紧急数据；

数据包在网络中经过的路由跳数；

网络中是否存在环路现象；

用户访问目标主机某服务的原始步骤。

8. 日志

日志视图记录网络中用户的高级网络运用，包括 HTTP 请求（网页浏览），邮件信息（通过 SMTP/POP3 进行的邮件收发），FTP 传输（通过 FTP 进行的数据上传下载）以及 DNS 分析（查看用户的 DNS 请求和响应情况），并可根据用户的需要将这些日志信息保存到硬盘以备查阅。其界面如图十所示，当前选定的是 HTTP 请求的日志视图。

概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表 报表

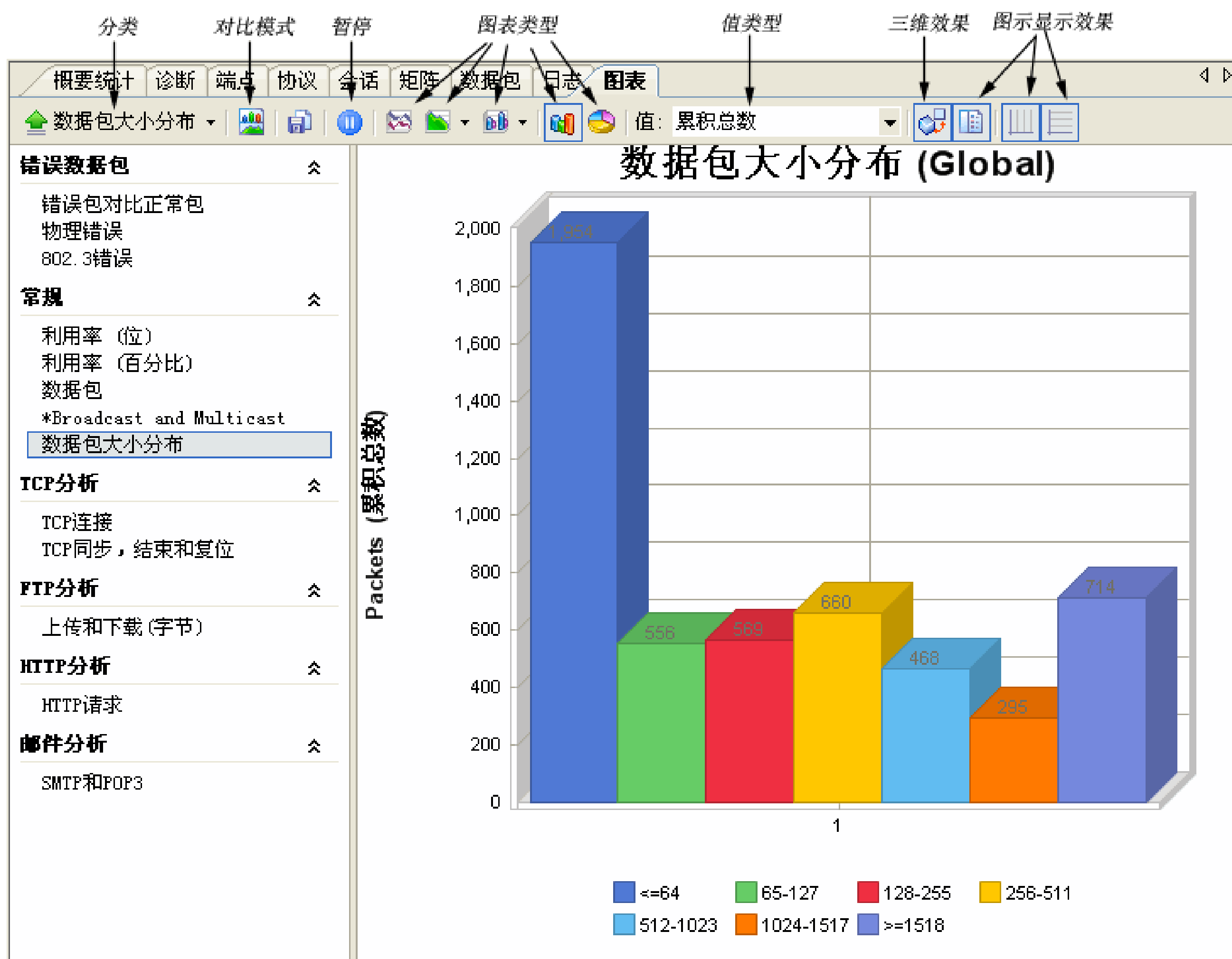
HTTP请求 日志: 41

日志
HTTP请求
邮件信息
FTP传输
DNS分析

时间	客户端	服务端	请求网址	请求方法	状态码
09:29:26	192.168.0.90:1551	tools.l.google.com:www-http	http://toolbar.google.com/...	GET	302
09:29:26	192.168.0.90:1552	www-china.l.google.com:www...	http://www.google.com/tool...	GET	200
09:29:45	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn/	GET	200
09:29:46	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:47	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:47	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:50	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:57	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304

9. 图表

图表功能为用户提供 2D 或者 3D 的时间趋势图和数据比较图，可以选择折线图、柱状图、面积图、饼图等多种形式，除了全局图表，也支持每个协议和网络端点的图表数据采集显示。



10.报表

八．工程设置

工程设置是对网络分析进行条件设置的地方，用户可以根据分析目的进行有选择的采集数据。工程设置主要包括以下几大类：

常规设置 – 主要设置数据包缓存

网络适配器 – 选择数据的采集方式

过滤器 – 选择分析的数据包范围

网络配置 – 可自定义网络节点，可按需要进行分组

日志设置 – 对邮件、FTP、HTTP、DNS 等高级分析模块的配置

诊断设置-- 对网络内的错误信息或故障信息进行自动提示

1. 工程设置－常规

这里主要是数据包缓存(Buffer)进行设置，数据包缓存在网络分析中可以起到高速缓冲存储数据的作用。

科来网络分析系统会将捕获到的数据包进行分析后，将数据保存在缓冲器中。只有当项目保存时，才将 Buffer 的数据保存在硬盘上。Buffer 的设置大小取决于所需要数据的多少和计算机内存的大小。Buffer 的大小应该低于一半的可用物理内存，一般开始先使用 16M 的 Buffer，如果需要时再增加。

例如： 一个 512M 的管理主机，运行操作系统和分析软件可能会占用 60M 内存，可用物理内存大概为 450M，除去其它的一些应用程序所占内存，可用物理内存大概不到 400M，那么 Buffer 最大的使用内存应该小于 200M。因为 Buffer 是独占使用，所以，我们还是尽量少划分内存作为 Buffer，一般 16M 可以满足大多数情况，流量大时，建议使用 64M 或 96M。

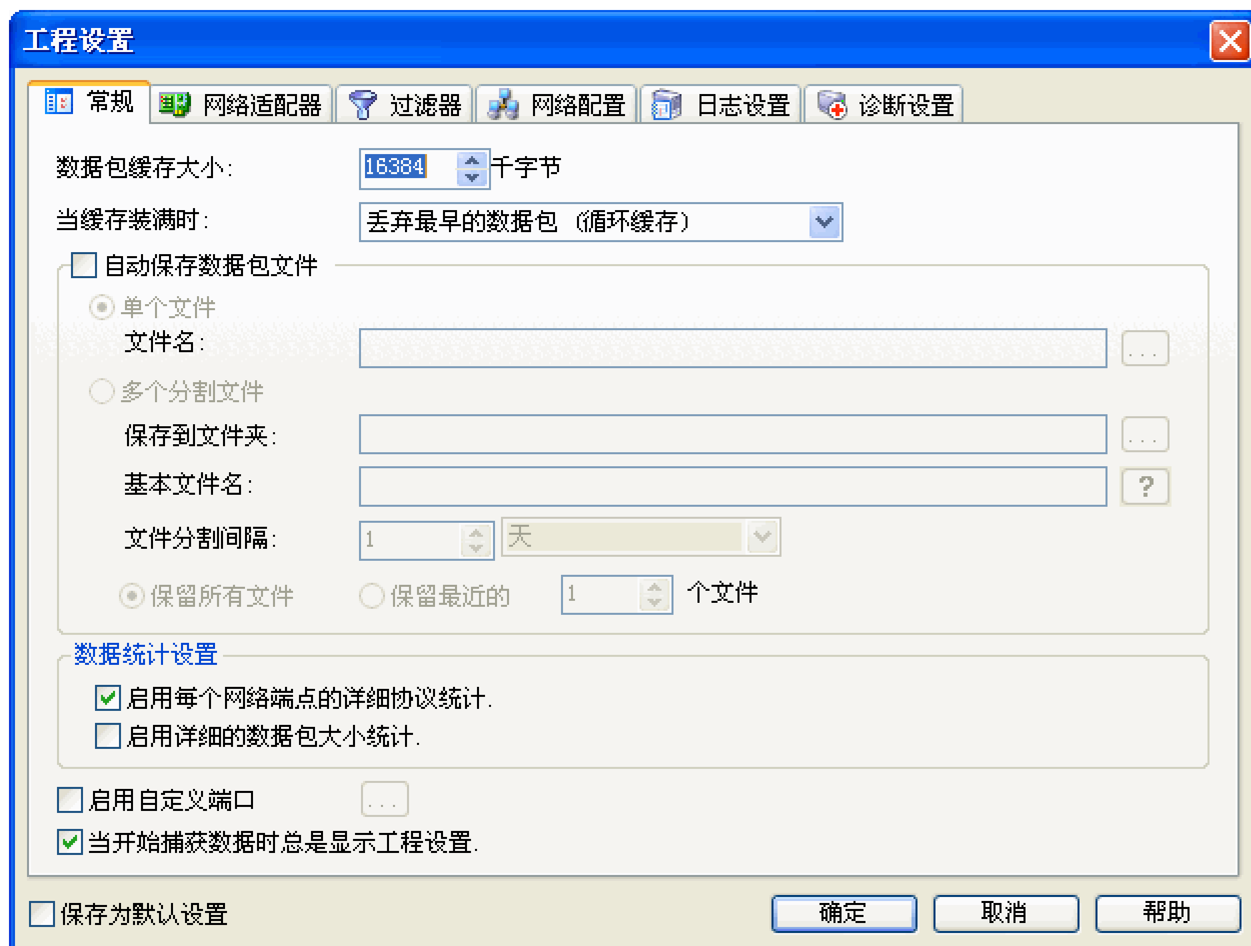
当缓存装满时，可选择以下处理方法：

丢弃最老的数据包 (Ring Buffer)
当被捕捉的数据包数量达到您设定的最大值时，本系统将会丢弃缓存中最早保存的数据包，然后添加新的数据包。

丢弃新捕获的数据包
当被捕捉的数据包数量达到您设定的最大值时，新捕获的数据包将在被分析模块分析后被丢弃而不会被保存在缓存中。

丢弃缓存内所有的数据包
当被捕捉的数据包数量达到您设定的最大值时，本系统将清空缓存然后再添加新的数据包。

停止捕捉数据包
当被捕获的数据包数量达到您设定的最大值时，本系统将停止捕捉和分析数据包，您将不能看到新捕获的数据。

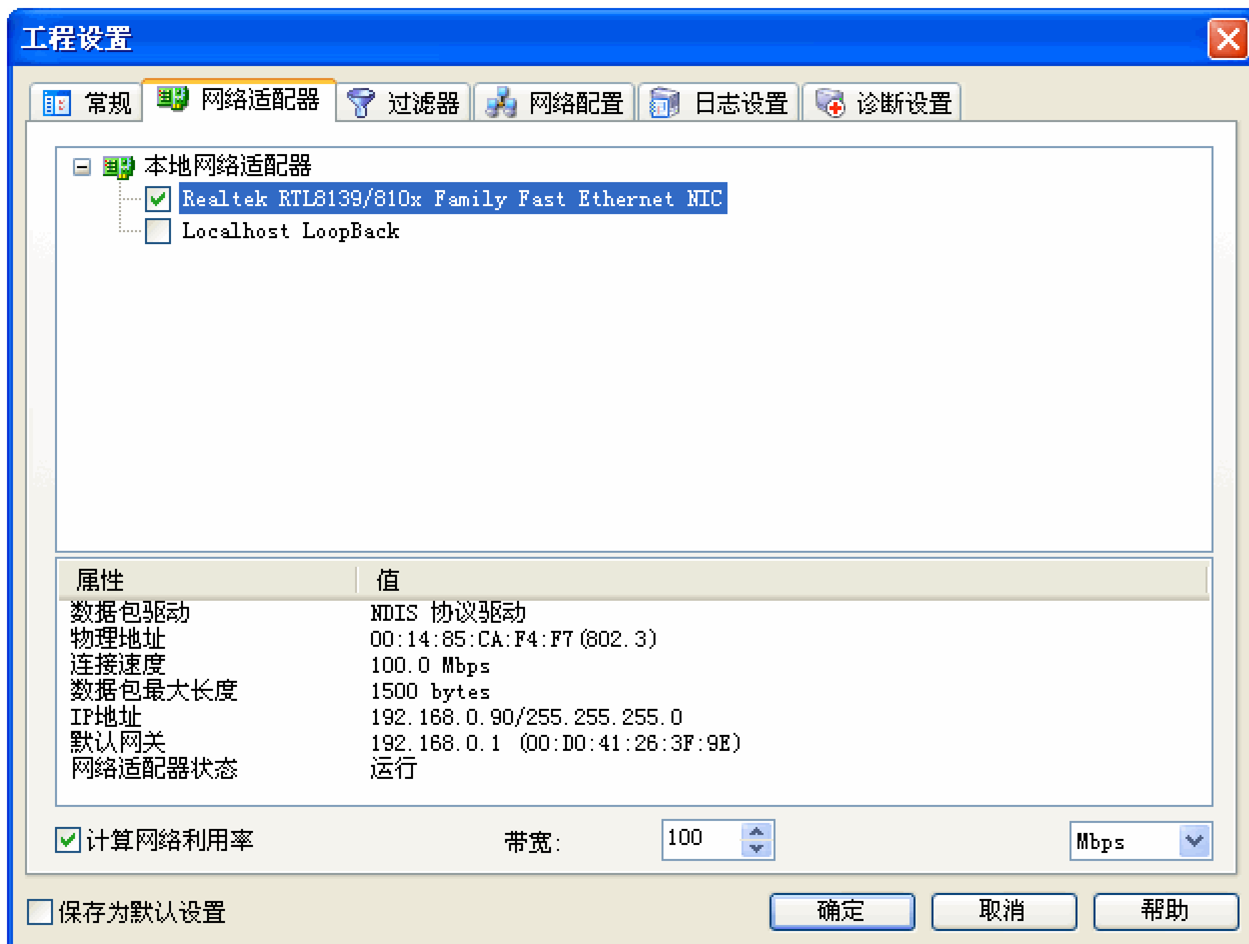


2. 工程设置－网络适配器

选择网络适配器，主要是选择数据的采集方式。

科来网络分析系统 6.4 支持以太网、拨号上网、本地环回方式的数据采集，并且也支持多网卡采集，用户可以选择一个网卡或多个网卡来捕获数据包。

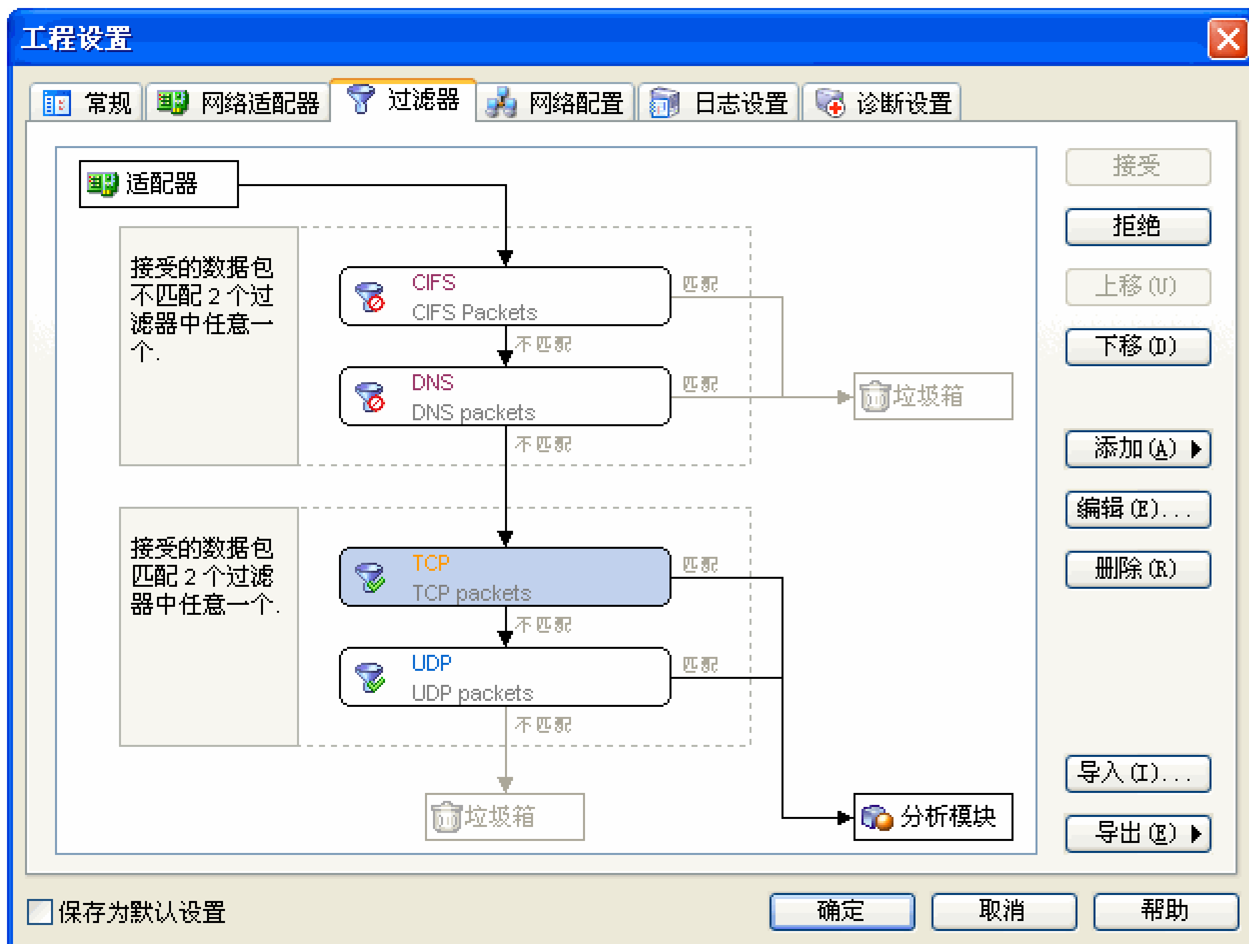
科来网络分析系统也能自动识别网卡的传输速度，默认以网卡的速度为网络带宽，用户也可以根据实际情况改变此值。如网卡虽然为 1000M，但内网的网线却是 100M，为了使统计更附合实际，可将带宽改为 100M。



3. 工程设置－过滤器

通过数据包过滤器列表页面您可以自定义捕捉数据包的过滤器。如果没有设定过滤器，科来网络分析系统将捕捉和分析所有数据包。

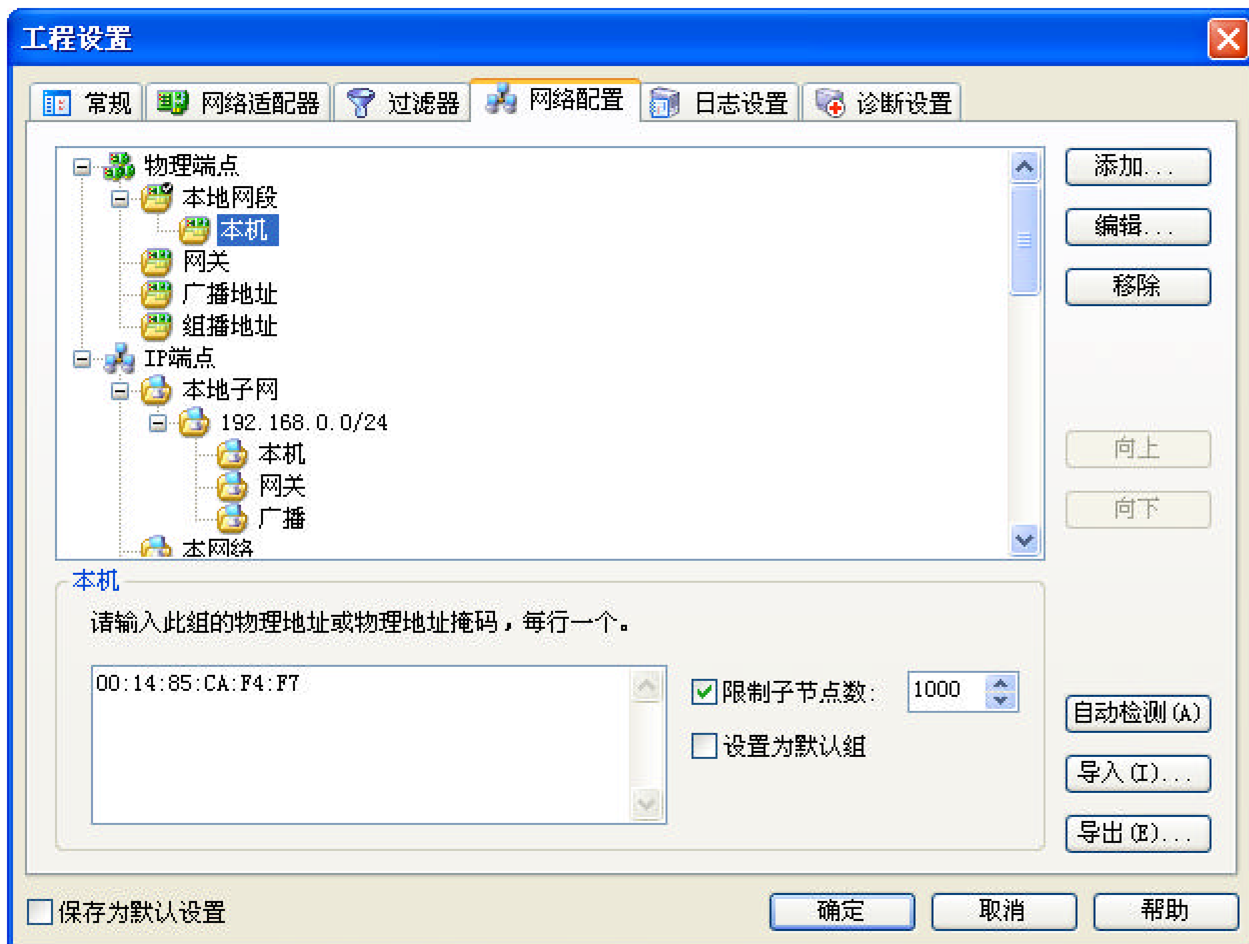
过滤器在科来网络分析系统 6.4 中被分为简单过滤器和高级过滤器。用户可以通过设置 IP、端口、协议、数据包值等条件来分离数据包。在过滤器列表中，可以通过“接受”☑、“排除”⊘等逻辑关系来组合过滤设置。



4. 工程设置－网络配置

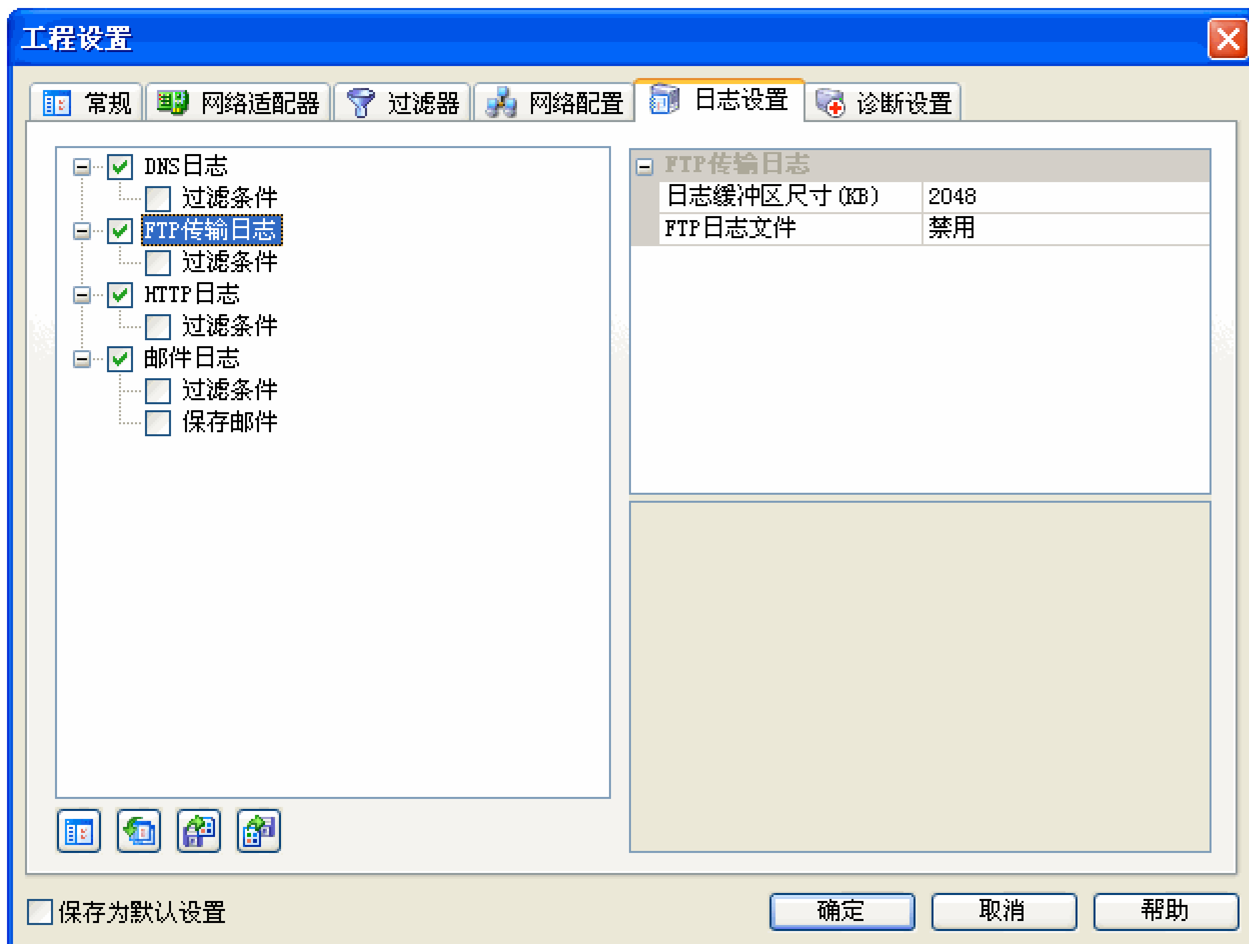
网络配置主要是自定义节点浏览器中 IP 节点和 MAC 节点。在 IP 节点和 MAC 节点按照网络数据的类型，定义了不同的组，用户可以很方便的查看本地数据、远程数据以及广播数据、组播数据。用户也可以根据需要添加、删除来规划自己的网络结构。例如，可以把不同网段分到不同 IP 组里，也可以按照部门建立不同的 IP 组。

科来网络分析系统 6.4 已经有一个默认的配置，点击自动检测，系统将对网络进行自动扫描，将 IP 节点和 MAC 节点自己检测出来。



5. 工程设置－日志设置

在工程设置里，也可以对网络分析模块进行配置。日志设置主要提供邮件分析、FTP、HTTP、DNS 分析。通过点击工具栏的图标，可打开 日志设置对话框。
在配置中，可以启用是否保存邮件，是否使用过滤器，以及端口和保存路径等。

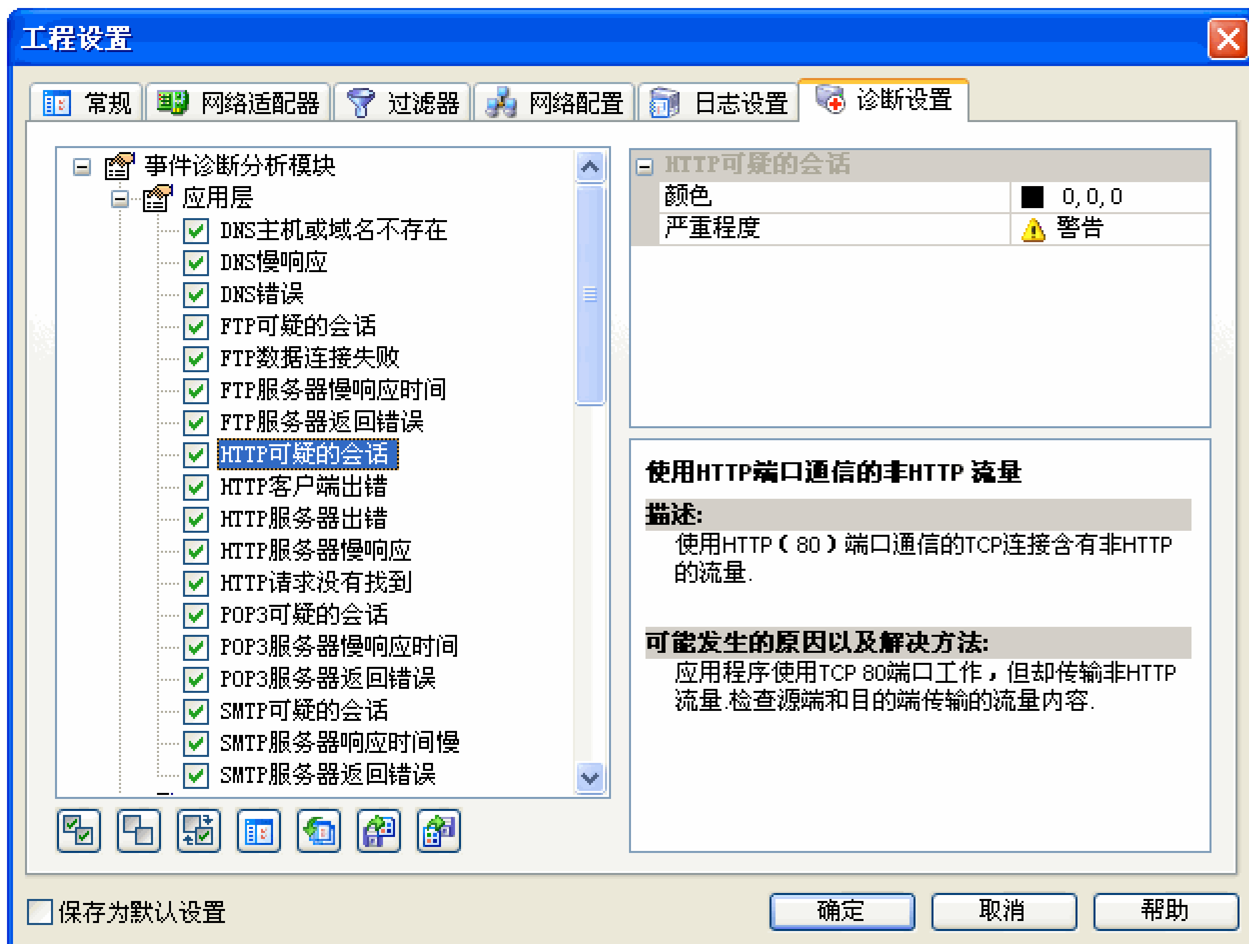


6．工程设置－诊断设置

诊断设置中，包含了系统内置的所有诊断事件，用户可以根据自身的网络情况，更改诊断事件的设置，如颜色、严重程度、条件阀值等。如果不想进行诊断的事件，用户也可以在列表中，取消该事件的诊断应用。

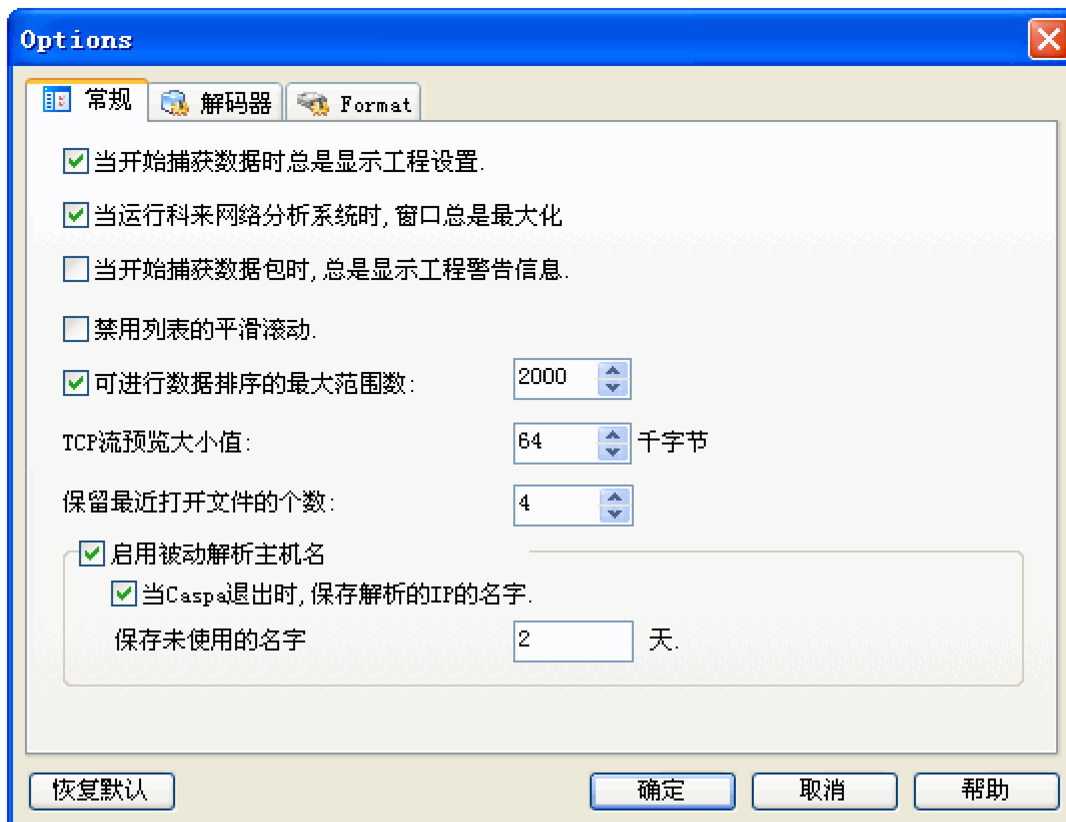
诊断设置中，所有的诊断事件都是以协议层来分类，即应用层、传输层、网络层、数据链路层。这样我们对于网络出现的故障，我们便能很快判断出是网络的哪一层出了问题。系统对每个诊断事件都提供了事件描述、可能发生的原因，以及可采取的解决方案，这些信息对故障的排除是非常有参考价值的。

对于诊断设置中的配置，我们可以通过导入导出来与其他人员共享；如果设置混乱了，你也可以采取恢复默认值。

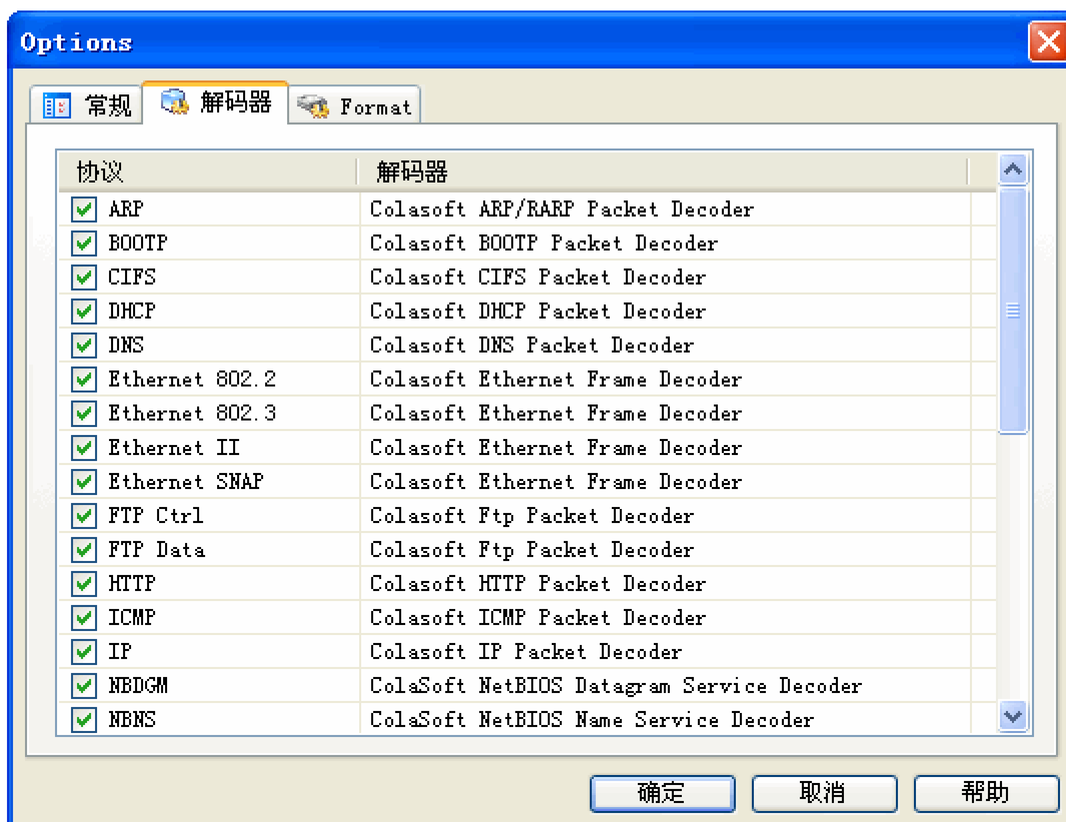


九.系统选项

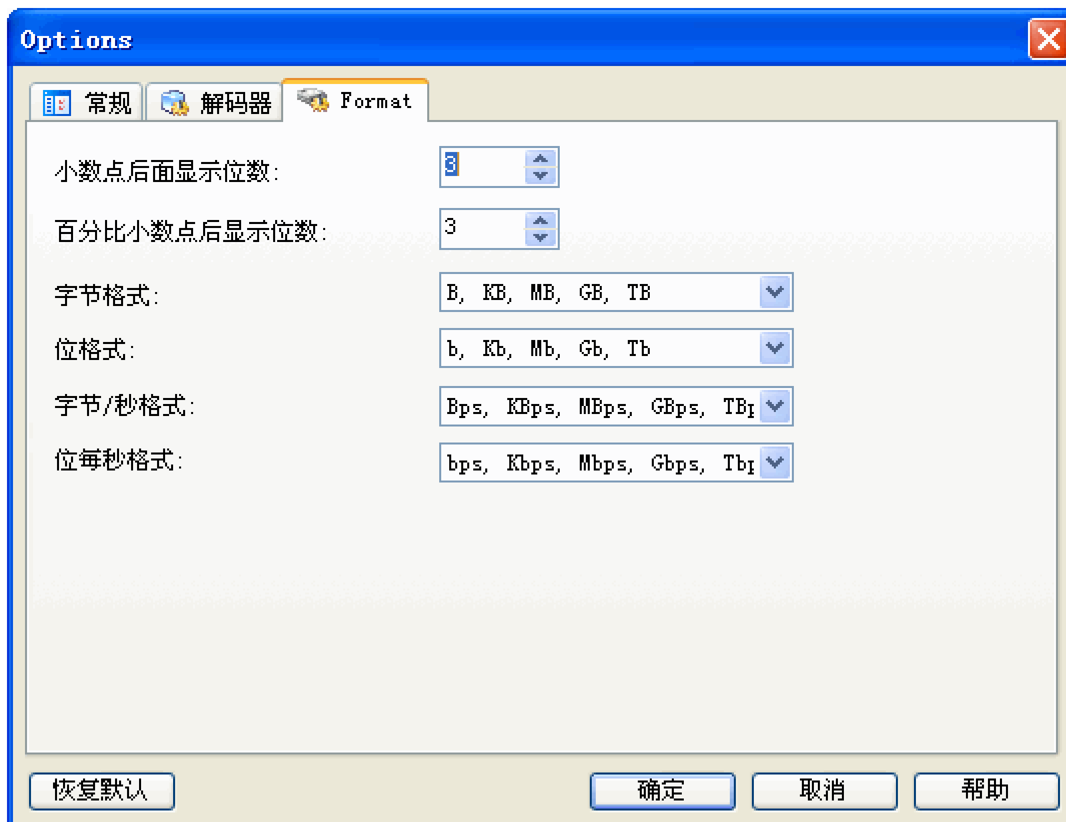
系统选项提供本系统的全局配置，并应用到所的工程项目中。用户可通过工具栏的图标打开系统选项对话框。系统选项包括常规配置、解码器配置、Format 格式配置。
常规配置中，提供一些数据的显示格式和操作配置，界面如下图。



解码器配置中提供科来网络分析系统 6.4 支持的解码模块，所有的解码器都按照模块化设计，用户可以任意选择和组合各种解码器。默认情况下，系统开启所有的解码模块对数据包进行解码 ，界面如下图。



Format 格式配置，用来配置系统视图中的显示格式，如小数点后面的显示位数，百分比小数点后显示位数等，界面如下图。



十.统计分析

统计分析是对网络进行实时监控，实时分析，并将统计结果自动展现在各个视图中，用户可以对统计分析结果进行复制、导出、打印、生成日志和生成报表等操作。

科来网络分析系统 6.4 中，统计分析得到极大加强。主要表现在：网络记录器多达上百种，增加了网络错误的监测，增加了数据包大小分布的统计，强加了利用率的分析，增加了协议树的拓展分析，增加了对图形统计。

统计分析包括：概要统计、端点统计、协议统计、会话统计、矩阵统计、图表统计和报表统计。

- **概要统计：提供的近百个统计计数器为用户提供非常详尽的统计信息，快照功能允许用户对特定时段的数据变化进行比较。概要统计不仅是全局的，每个网络协议和网络端点都有自己的概要统计，用户可以开启多个窗口，比较不同协议或端点之间的概要统计。**

- **端点统计：是网络分析重要组成部份，科来网络分析系统将分为物理端点和 IP 端点，通过网络端点统计分析功能，用户可以快速找定位通讯量最大的 IP 端点和物理端点。系统还支持每个网络协议的端点流量明晰统计排名，比如用户可以知道 HTTP 协议下前 5 个 IP 端点。**

- **协议统计：遵循 OSI 七层协议分析，根据实际的网络协议封装顺序，层次化得展现给用户，每个协议有自己的色彩，除了全局的协议统计，还可提供每个网络端点下的协议统计数据。**

- **会话统计：提供物理地址、IP 地址、TCP 连接、UDP 会话来统计网络中的会话信息，并在下方的子窗口中显示当前选定会话的数据包等信息。通过查看每条会话，我们可以统计其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。我们可以通过这些信息确定出当前网络中某个会话的通讯情况。**

- 矩阵统计：可对网络中通讯的节点和会话进行详细统计，用户可以通过不同的统计类型来查看矩阵视图，此外，用户还能自定义显示选项。

- 图表统计：为用户提供 2D 或者 3D 的时间趋势图和数据比较图，可以选择折线图、柱状图、面积图、饼图等多种形式，除了全局图表，也支持每个协议和网络端点的图表数据采集显示。

- 报表统计：实时为用户选中的节点生成报表，选成前，用户可以通过报表选项，确定生成的报表项，待报表生成后，用户还可以将生成的报表以 html 格式保存到磁盘中。

十一. 诊断

专家诊断是科来网络分析系统 6.4 的重要功能，可以将捕获到的数据进行智能化的分析，对网络内的错误信息或故障信息，进行自动提示，用户可以不必去了解数据包的详细内容，便可以从专家诊断模块中获得网络内的错误和故障分析。

诊断视图分为上下两个视图，上面的视图是按照 OSI 七层协议对错误信息进行分组，目前产品支持四个层次的故障诊断：应用层、传输层、网络层、数据链路层。用户可以分别查看不同协议层都有哪些网络错误和故障。而网络错误和故障都有安全级别的划分，有的是普通信息提示，有的是严重的错误警告，如下表所示：

安全级别	图标	描述
消息		普通信息通知，只是用来记录某个事件，并没有网络错误。
注意		对网络事件或特定事件进行提示，需要用户引起重视的内容。
警告		对错误或故障进行警告提示，用户应该及时处理。
危急		这是对严重错误或严重故障进行提示，用户需要及时处理。

诊断视图简图如下所示：

另存为 显示操作 刷新

概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表

名称	计数
所有的诊断事件	34
传输层	34
TCP太多重传	7
TCP连接被拒绝	1
TCP连接被重置	3
TCP重传数据包	15
TCP重复的连接尝试	8

事件 参考信息

0 0 7 0 TCP太多重传: 7

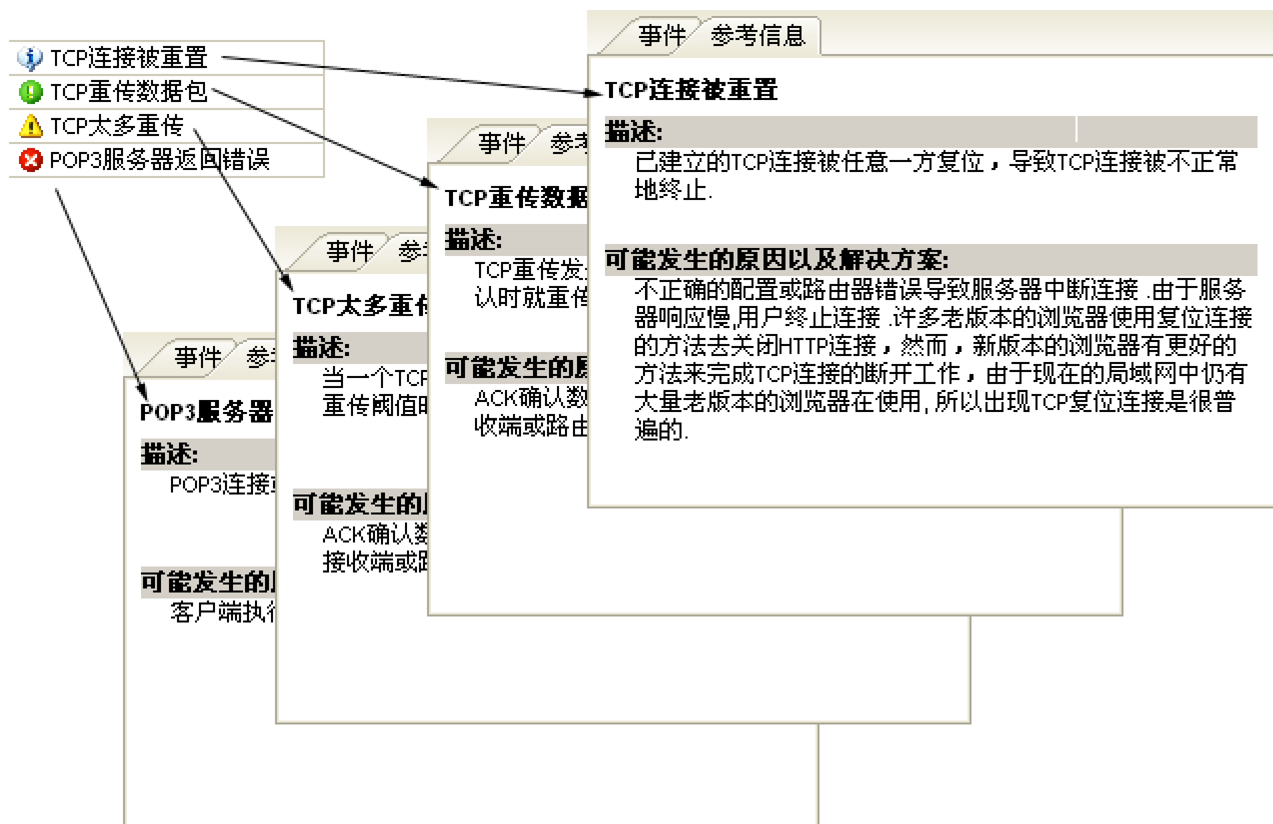
严重程度	协议层	事件	源	目标
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90
	Transport Layer	TCP太多的重传数据包	207.46.2.101	192.168.0.90

事件详细信息 事件参考信息

1．诊断参考

对应每一种诊断事件，专家诊断模块都提供事件的解释，起因，以及可能采用的解决方案，管理人员可以很方便快速的了解当前的网络状况，并根据诊断的参考信息做出快速响应，及时的排除网络错误和故障问题。

下图是对其中几种网络事件的参考信息：



2. 参考信息－应用层

下面是应用层的事件诊断的对应信息。包括事件名称、事件描述、严重等级、可能的原因及解决方法：

事件	描述	严重等级	可能的原因及解决方法
DNS 主机或域名不存在	用户所请求的域名不存在	信息	请求的域名不存在或域名输入错误。
DNS 主机慢响应	DNS 服务器的平均响应时间大于或等于 DNS 主机慢响应阈值。	注意	DNS 服务器过载。
DNS 错误	用户所请求的主机或域名没有成功返回	注意	查询格式错、服务器失败、未实现、拒绝、预留。
HTTP 服务器响应太慢	HTTP 服务器的平均响应时间大于或等于 HTTP 慢响应预设阈值。	注意	Web 服务器过载。
HTTP 验证失败	HTTP 客户端发起的验证请求失败导致验证被拒绝。	警告	登录时使用了错误的用户名或密码。
使用 HTTP 端口通信的非 HTTP 流量	使用 HTTP（80）端口通信的 TCP 连接含有非 HTTP 的流量	警告	应用程序使用 TCP 80 端口工作，但却传输非 HTTP 流量 。 检查源端和目的端传输的流量内容。 当客户端请求的页面未找到时 HTTP 服务器返回此错误（404）。
HTTP 请求页面未找到	当客户端请求的页面未找到时 HTTP 服务器返回此错误（404）。	消息	用户输入了无效的网址。 Web 服务器连接被中断。 HTTP 服务器返回一个除 404 以外的 4xx 代码标识一个客户端错误，表示客户端请求页面未找到。

HTTP 客户端错误	HTTP 服务器返回一个除 404 以外的 4xx 代码标识一个客户端错误，表示客户端请求页面未找到。	消息	HTTP 服务器返回一个 5XX 的代码标识服务器错误，客户端的请求通常是正确的。
HTTP 服务器错误	HTTP 服务器返回一个 5XX 的代码标识服务器错误，客户端的请求通常是正确的。	警告	POP3 客户端登陆服务器失败。
POP3 登陆失败	POP3 客户端登陆服务器失败。	警告	用户名或密码错误。
POP3 服务器响应太慢	POP3 服务器的平均响应时间大于或等于 POP3 慢响应预设阈值。	注意	POP3 服务器过载。
使用 POP3 端口通信的非 POP3 流量	使用 POP3（110）端口通信的 TCP 连接含有非 POP3 的流量	警告	应用程序使用 TCP 110 端口工作，却传输了非 POP3 流量。 检查源端和目的端传输的流量内容。
POP3 服务器返回错误	POP3 连接或请求在 TCP 连接成功建立后被 POP3 服务器拒绝。	危急	客户端执行了错误的命令。 服务器忙。 SMTP 客户端登录服务器失败。
SMTP 登录失败	SMTP 客户端登录服务器失败。	警告	用户名或密码错误。
SMTP 服务器响应太慢	SMTP 服务器的平均响应时间大于或等于 SMTP 慢响应预设阈值。	注意	SMTP 服务器过载。
使用 SMTP 端口通信的非 SMTP 流量	使用 SMTP（25）端口通信的 TCP 连接含有非 SMTP 的流量。	警告	应用程序使用 TCP 25 端口工作，却传输了非 SMTP 流量。 检查源端和目的端传输的流量内容。
SMTP 服务器返回错误	SMTP 连接或请求在 TCP 连接建立后被 SMTP 服务器拒绝。	危急	客户端执行了错误的命令。 服务器忙。 FTP 客户端登陆服务器失败。
FTP 登陆失败	FTP 客户端登陆服务器失败。	警告	用户名或密码错误。
FTP 服务器响应太慢	FTP 服务器的平均响应时间大于或等于 FTP 慢响应预设阈值。	注意	FTP 服务器过载。
使用 FTP 端口通信的非 FTP 流量	使用 FTP 控制端口（21）的 TCP 连接含有非 FTP 的流量。	警告	应用程序使用 TCP 21 端口工作,却传输了非 FTP 流量。 检查源端和目的端传输的流量内容。
FTP 服务器返回错误	FTP 连接或请求在 TCP 连接成功建立后被 FTP 服务器拒绝。	危急	客户端执行了错误的命令。 服务器忙。
FTP 数据连接失败	FTP 数据连接已经初始化,但创建失败。	警告	防火墙封堵了 FTP 数据连接端口。 FTP 服务器不接受被动(PASV)模式的 FTP 数据连接 Telnet 客户端登陆服务器失败。

3．参考信息－传输层

下面是传输层的事件诊断的对应信息。包括事件名称、事件描述、严重等级、可能的原因及解决方法：

事件	描述	严重等级	可能的原因及解决方法
TCP 复位连接	已建立的 TCP 连接被任意一方复位，导致 TCP 连接被不正常地终止。	消息	不正确的配置或路由器错误导致服务器中断连接 由于服务器响应慢,用户终止连接 许多老版本的浏览器使用复位连接的方法去关闭 HTTP 连接，然而，新版本的浏览器有更好的方法来完成 TCP 连接的断开工作。 由于现在的局域网中仍有大量老版本的浏览器在使用，所以出现 TCP 复位连接是很普遍的。
TCP 复位非活动连接	已建立的 TCP 连接达到复位非活动连接的阈值后被任意一方复位。	消息	由于 TCP 客户端空闲时间太长,TCP 服务器复位此客户端连接 。 许多老版本的浏览器使用复位连接的方法去关闭 HTTP 连接。
TCP 重复连接尝试	客户端多次试图建立 TCP 连接。	警告	客户端发往服务器的 SYN 包和服务器返回的 ACK 包被防火墙阻止 。 客户端请求了服务器未提供的服务。
TCP 连接被拒绝	客户端尝试初始化 TCP 连接，但被目标主机拒绝。	警告	客户端请求了服务器未提供的服务。 服务器没有足够的可用资源以接受新的连接。
TCP 重传	TCP 重传发生在当发送端没收到接收端对某数据包的 ACK 确认时就重传该数据包。	注意	ACK 确认数据包通过较慢的路由进行传输 。 网络负载过大。 接收端或路由器过载。
TCP 太多重传	当一个 TCP 连接中的重传数据包百分比大于或等于 TCP 太多重传阈值时，科来网络分析系统将给出 TCP 太多重传警告。	警告	ACK 确认数据包通过较慢的路由进行传输。 网络负载非常大。 接收端或路由器过载。
TCP 快速重传	在小于重传阈值时间的情况下，TCP 发送端就重传数据包。	警告	确认数据包通过较慢的路径进行传输。 网络负载过大。 接收端或路由器过载。
TCP 校验和错误	TCP 报头和(或)数据校验和有错。发送端在发送数据包前计算校验和并将校验和的值写入数据包，接收端收到数据包后重新计算数据包的校验和,如果两个值不相同表示出错。	警告	网络中某设备存在故障 。 如果所有本地数据包的校验和均显示为错误，这可能是因为启用了不计算校验和的功能。 当该功能可用时,适配器就去执行计算 CRC 的过程,Windows 的 TCP/IP 栈不计算 IP 和 TCP 校验和,并以 0x0000 标识，科来网络分析系统会在每一个输出包到达适配器之前收集它们的副本。 要解决此问题，你需要在网络适配器的高级设置对话框中禁用适配器的卸掉传输 TCP 校验和和卸掉传输 IP 校验和选项。
TCP 零窗口持续时间太长	TCP 连接中任一方零窗口的持续时间大于或等于零窗口阈值所设定的时间。	警告	接收端非常繁忙 。 接受端的网络缓冲区不够。 应用程序的某些行为间接导致零窗口时间太长,例如应用程序可能会等待其它一些事件的发生或者没有释放帧缓冲区。 应用程序处理速度太慢.

TCP 慢应答	TCP 连接中 ACK 数据包的响应时间超过 TCP 连接慢响应阈值+平均响应时间。	警告	确认数据包通过较慢的路由进行传输 。 网络负载过大。 接收端或路由器过载
TCP 窗口冻结	三个或更多连续的数据包 TCP 窗口大小保持不变，且此窗口尺寸小于最大窗口阀值所设定的百分比。	警告	TCP 源端网络应用程序缓冲区不足
TCP 窗口过小	TCP 窗口尺寸小于最大窗口阀值所设定的百分比。	消息	TCP 源端网络应用程序缓冲区不足
TCP 端口扫描	一个本地或远程工作站扫描网络中打开的 TCP 端口。	警告	端口扫描是网络入侵的标志。
UDP 校验和错误	UDP 报头和(或)数据校验和有错。发送端在发送数据包前计算校验和并将校验和的值写入数据包，接收端收到数据包后重新计算数据包的校验和,如果两个值不相同表示出错。	警告	网络中某设备存在故障.

4．参考信息－网络层

下面是网络层的事件诊断的对应信息。包括事件名称、事件描述、严重等级、可能的原因及解决方法：

事件	描述	严重等级	可能的原因及解决方法
ICMP 目标不可达	工作站收到一个 ICMP 目标不可达消息	警告	目标网络不存在
ICMP 主机不可达	工作站收到一个 ICMP 主机不可达消息	警告	目标主机不存在.
ICMP 网络不可达	工作站收到一个 ICMP 网络不可达消息	警告	目标网络不存在.
ICMP 参数错误	工作站发送一个 ICMP 消息标示参数错误	警告	
ICMP 端口不可达	工作站收到一个 ICMP 端口不可达消息	警告	工作站请求的目标端口在目标主机上没有打开
ICMP 主机重定向	工作站收到一个代码为 1 的 ICMP 重定向消息（重定向数据报到主机）	警告	路由器发送消息通知工作站存在一条到达目的地更好的路由
ICMP 网络重定向	工作站收到一个代码为 0 的 ICMP 重定向消息（重定向数据报到网络）	警告	路由器发送消息通知工作站存在一条到达目的地更好的路由
ICMP 源抑制	工作站收到一个 ICMP 源抑制消息	警告	发送消息的工作站可能死机或重启.
IP 报头无效校验和	IP 报头校验和有错。 发送端在发送数据包前计算校验和并将计算结果写入数据包，当接收端收到数据包后重新计算数据包的 IP 报头校验和,如果两个值不相同就表示出错。	警告	网络中某设备存在故障.
IP 生存周期太短	IP 数据包的 TTL 字段的值为 0 或 1 表示该数据包将过期，即将被丢弃。	注意	网络中某路由器的路由表有错 网络环路 源主机在开始传输数据包时使用了低的 TTL 值

			可尝试定位原始数据包来源
IP 段丢失	一个 IP 数据包被分段传输时丢失了其中一个分段，这通常会导致重传该丢失的分段。	注意	IP 分段被交换机或路由器丢弃 网络流量过大
IP 零广播地址	IP 数据包中使用了旧的广播地址 0.0.0.0	注意	这是一个已经废弃了的 TCP/IP 广播地址。 检查源端点应用程序是否发送了此数据包
IP 地址冲突	有多个 MAC 物理地址配置了同一个 IP 地址	警告	新分配的 IP 地址在网络中不是唯一的，它与网络中已存在的 IP 地址发生了冲突 动态分配网络地址不正确 如果这些 MAC 地址是来自路由器的，则是正常情况。

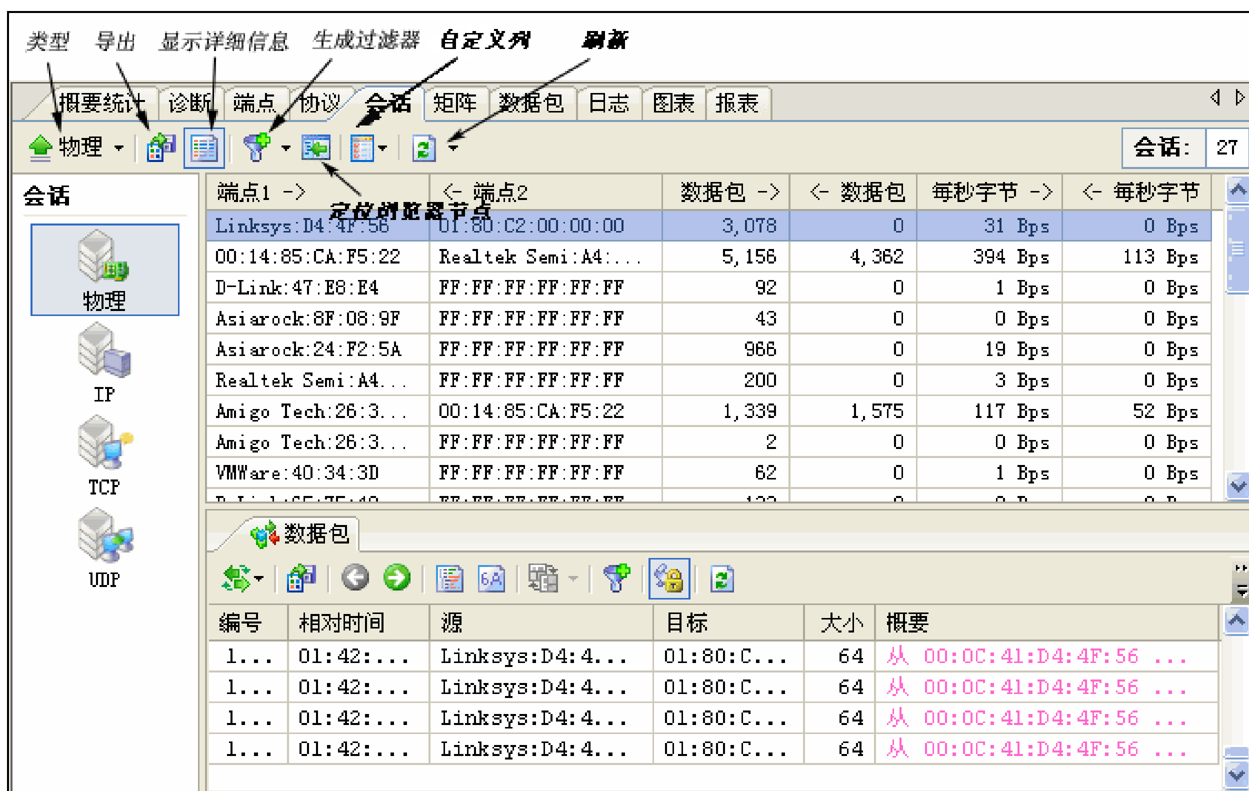
5．参考信息－数据链路层

下面是数据链路层的事件诊断的对应信息。包括事件名称、事件描述、严重等级、可能的原因及解决方法：

事件	描述	严重等级	可能的原因及解决方法
太多无请求的 ARP 响应	当来自某一物理节点的 ARP 响应超过或等于无请求响应阀值预设的百分比，科来网络分析系统将会发出此警告。	警告	检查源端和目的端物理节点可能存在 ARP 欺骗。
ARP 请求风暴	ARP 每秒请求数据包数量超过 ARP 请求阈值设定的值，表示网络中发生了 ARP 请求风暴。	警告	检查 ARP 数据包的源主机程序是否在大量发送 ARP 请求。
ARP 扫描	工作站通过 ARP 请求扫描网络地址。	警告	检查发送 ARP 数据包的源主机是否有程序在进行扫描。

十二.会话

会话视图功能是科来网络分析系统 6.4 在新增的一个重要功能，通过会话视图我们可以知道当前网络的会话情况。如图所示，



会话视图提供物理地址、IP 地址、TCP 连接、UDP 会话用来显示网络中的会话信息。并在下方的子窗口中显示当前选定会话的数据包等信息。

通过查看每条会话，我们可以统计其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。我们可以通过这些信息确定出当前网络中某个会话的通讯情况。

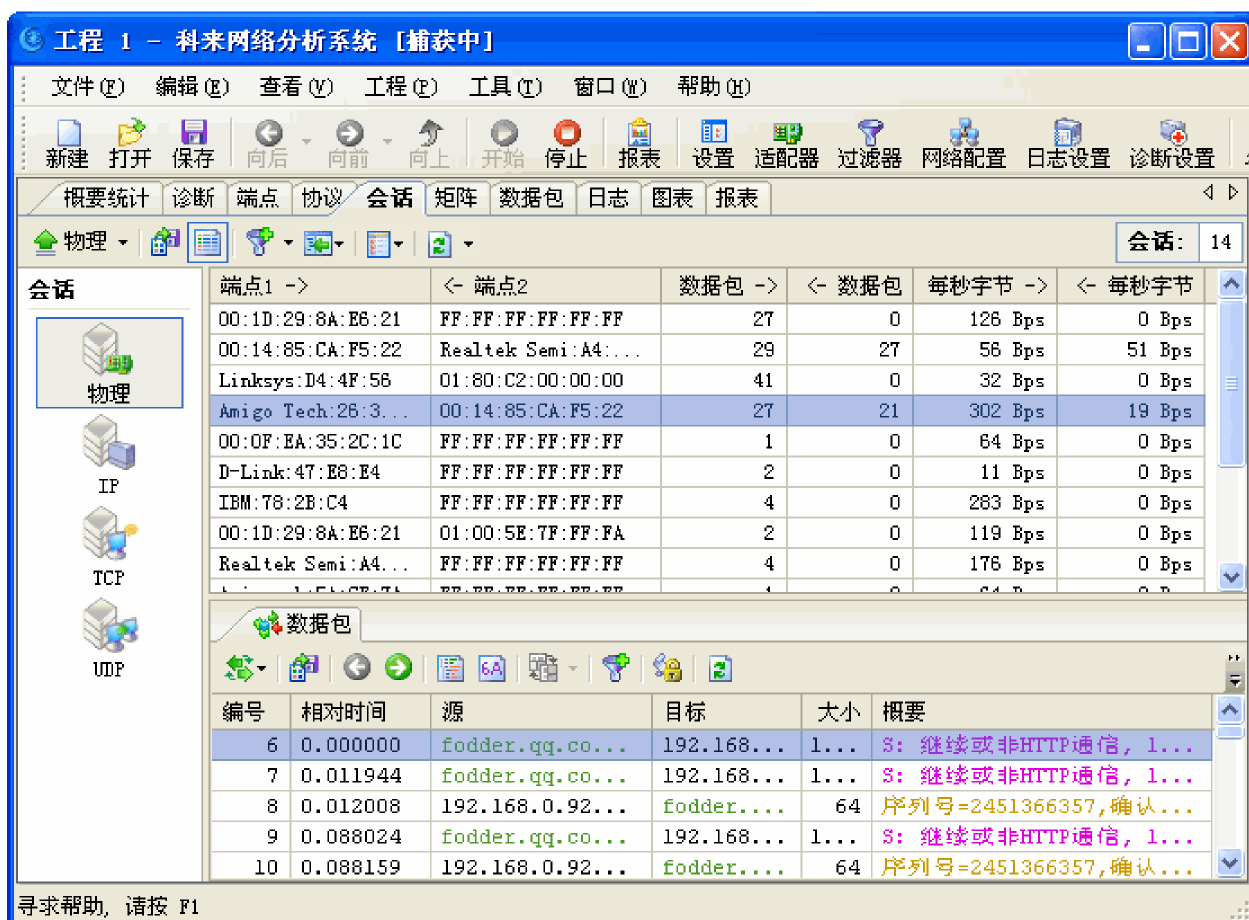
通过对会话视图的查看，管理人员可以：

- 设定显示选项，自定义要查看的数据列
- 双击打开新窗口查看会话细节
- 通过 Page UP 和 Page Down 来浏览前后连接
- 通过该会话生成过滤器
- 导出端点对数据
- 定位该会话所在节点
- 将 MAC 地址或 IP 地址添加到名字表
- 使用滚屏功能始终显示最新的会话

1. 物理地址

物理地址会话视图中，显示网络中物理地址之间会话的信息，可统计其源物理地址、目标物理地址、该连接收发的数据包及这些数据包的大小等信息。 并在下方的子

窗口中显示当前选定物理地址会话的原始数据包信息，通过这些信息，我们可以确定出当前网络中物理地址之间的通讯情况，如图所示。



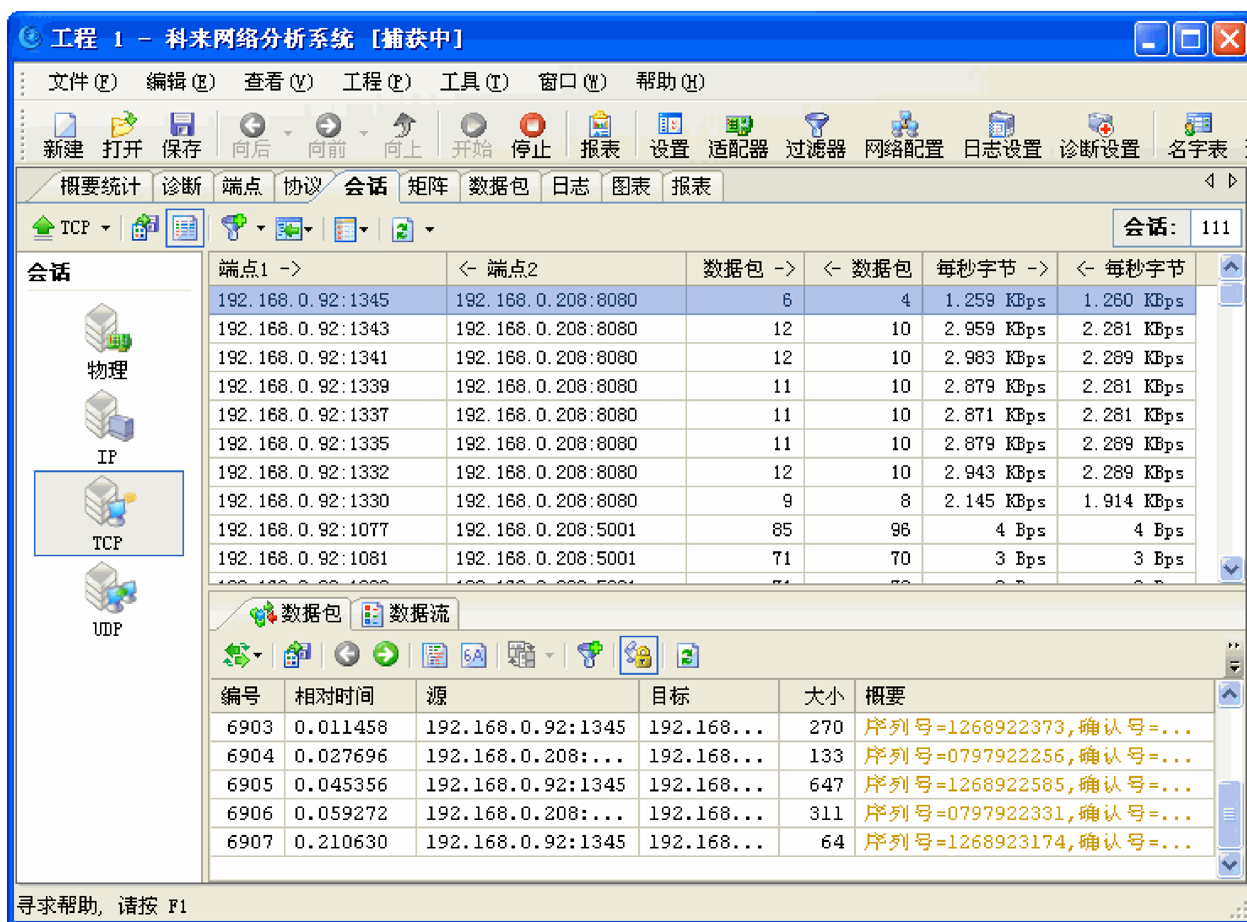
2. IP 地址

IP 地址会话视图中，显示网络中 IP 地址会话的信息，对于每条 IP 地址会话,都可统计其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。 并在下方的子窗口中显示当前选定的 IP 地址会话的原始数据包信息。通过这些信息，我们可以确定出当前网络中 IP 地址会话的情况，如图所示。



3. TCP 连接

TCP 连接会话视图显示当前网络活动状态，提供从整体到端点的 TCP 连接情况分析，即时的 TCP 流重组功能。



TCP 连接视图中，显示网络中 TCP 连接的信息，对于每条 TCP 会话,都可统计其源地址、目标地址、该连接收发的数据包及这些数据包的大小等信息。 并在下方的子窗口中显示当

前选定 TCP 连接的原始数据包信息、TCP 数据流重组信息。通过这些信息，我们可以确定出当前网络中 TCP 连接的情况，如：

查看两台主机之间的通讯内容；

网络中是否存在 TCP 端口扫描攻击；

网络中是否存在基于 TCP 协议的服务的账户用户名密码破解攻击；

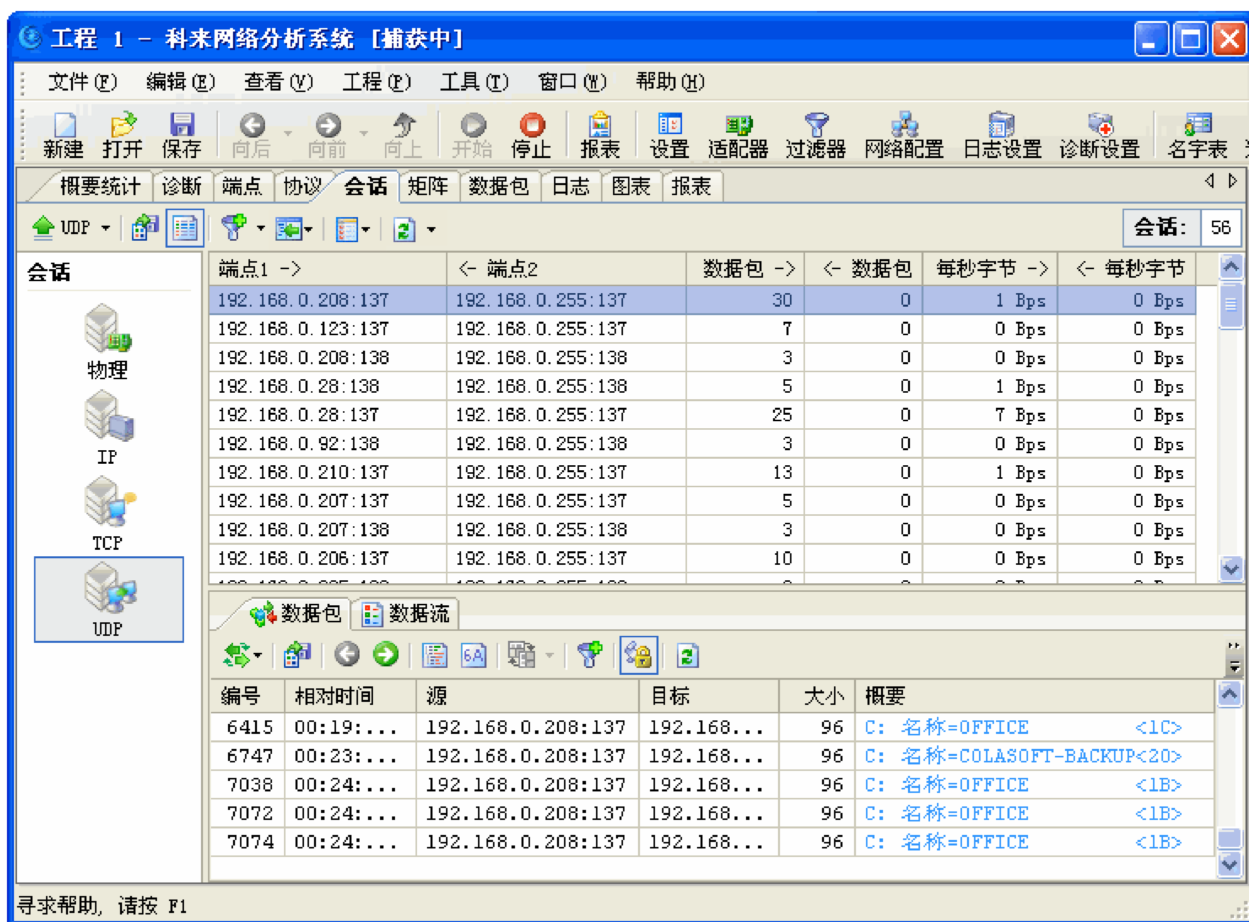
网络中是否存在邮件蠕虫病毒攻击；

网络中是否存在长时间连接且流量小的 TCP 连接（QQ/MSN 等程序使用 HTTP 代理即为此现象）。

下方的 TCP 数据流重组，可以方便地得出当前选定连接的原始操作信息，通过 TCP 连接的原始信息，我们可以确定这些 TCP 通讯的内容、步骤，并断定此连接是否正常。其界面如图所示。

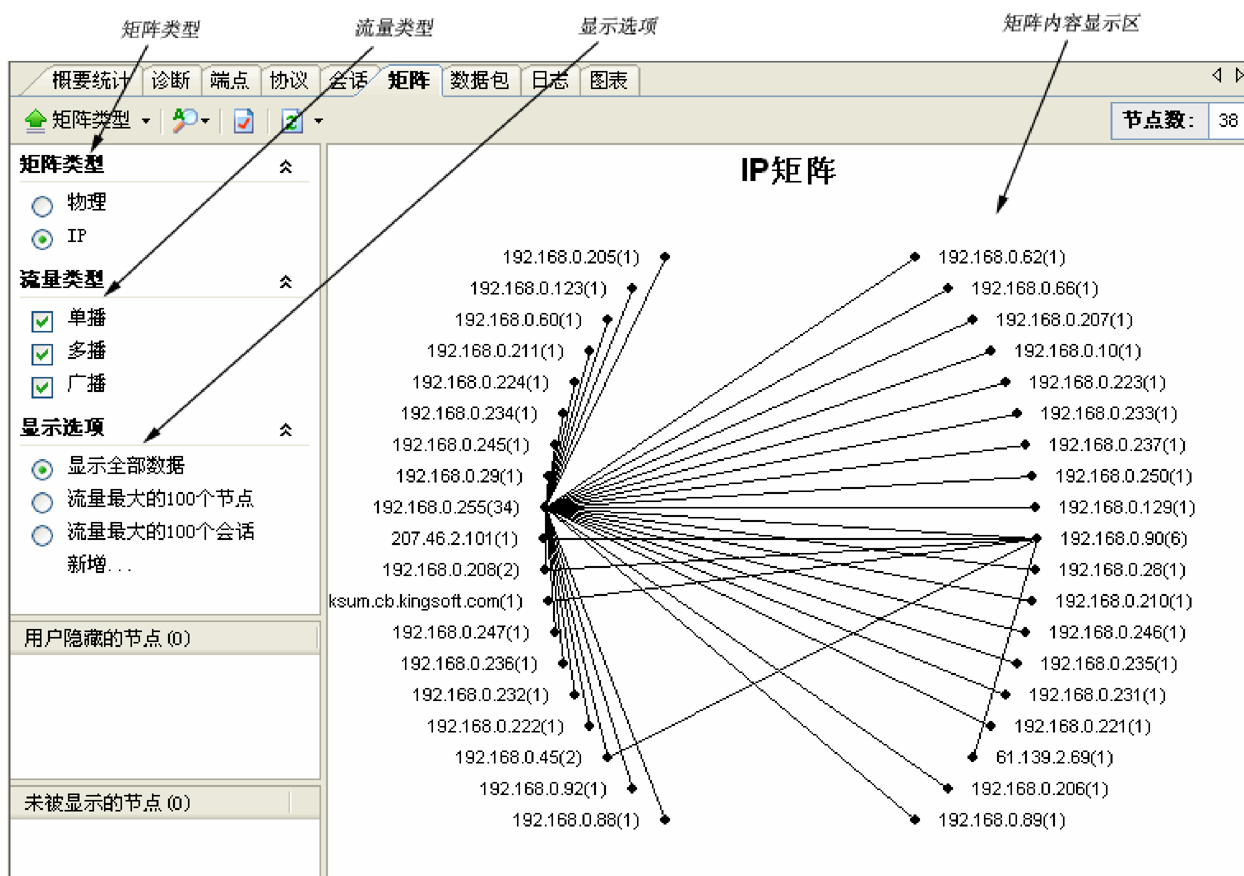
4. UDP 会话

UDP 会话图显示当前网络活动状态，提供从整体到端点的 UDP 会话情况分析，即时的 UDP 流重组功能。



十三.矩阵

科来网络分析系统 6.4 的提供的矩阵视图，可对网络中通讯的节点和会话进行详细统计，其界面如下图所示。



通过矩阵视图，我们可了解到以下信息：

整个网络通讯的节点信息；

整个网络通讯的会话信息；

某台物理主机的通讯节点信息；

某台 IP 主机的通讯会话信息；

某台物理主机的通讯节点信息；

某台 IP 主机的通讯会话信息；

某条会话的主机信息；

矩阵类型有物理地址和 IP 地址两种，同时只能选择查看一种类型的矩阵，系统默认选中的是 IP。

物理地址：根据物理地址（MAC 地址）节点显示矩阵内容；

IP 地址：根据 IP 地址节点显示矩阵内容。

流量类型有单播、多播和广播三种，可以同时选择查看一种或多种类型的流量，系统默认将三种流量全部选中。

单播：目标地址和源地址都是单播地址的流量，称为单播流量，选中单播后，右边的矩阵内容显示区会显示网络中单播流量的矩阵信息；

多播：目标地址或源地址是多播地址的流量，称为多播流量，有时也称为组播流量，选中多播后，右边的矩阵内容显示区会显示网络中多播流量的矩阵信息；

广播：目标地址或源地址是广播地址的流量，称为广播流量，选中广播后，右边的矩阵内容显示区会显示网络中广播流量的矩阵信息。

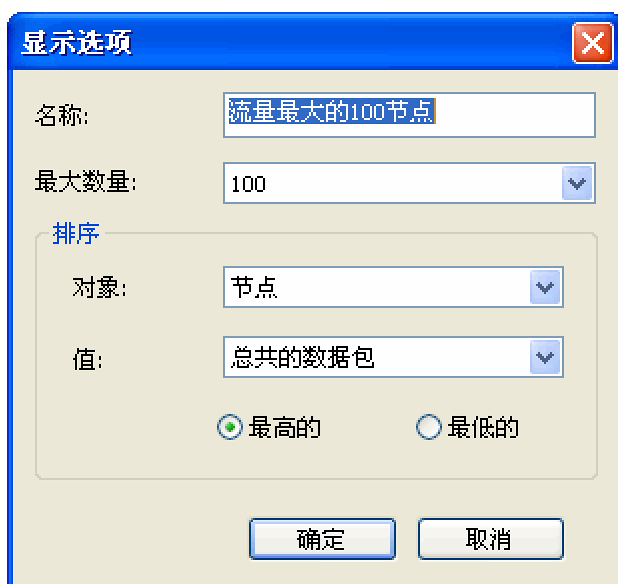
显示类型默认有"显示全部数据"、"流量最大的 100 个节点"、"流量最大的 100 条会话"、 三个选项和一个"新增..."功能，选项类型之间是单选。

显示全部数据：显示符合矩阵类型、流量类型设定的所有矩阵信息；

流量最大的 100 个节点：显示符合矩阵类型、流量类型设定的流量最大的 100 个节点的矩阵信息；

流量最大的 100 条会话：显示符合矩阵类型、流量类型设定的流量最大的 100 条会话的矩阵信息；

New：添加自定义的显示过滤条件，单击后弹出如下所示的图，用户可根据自己的需要进行设定。

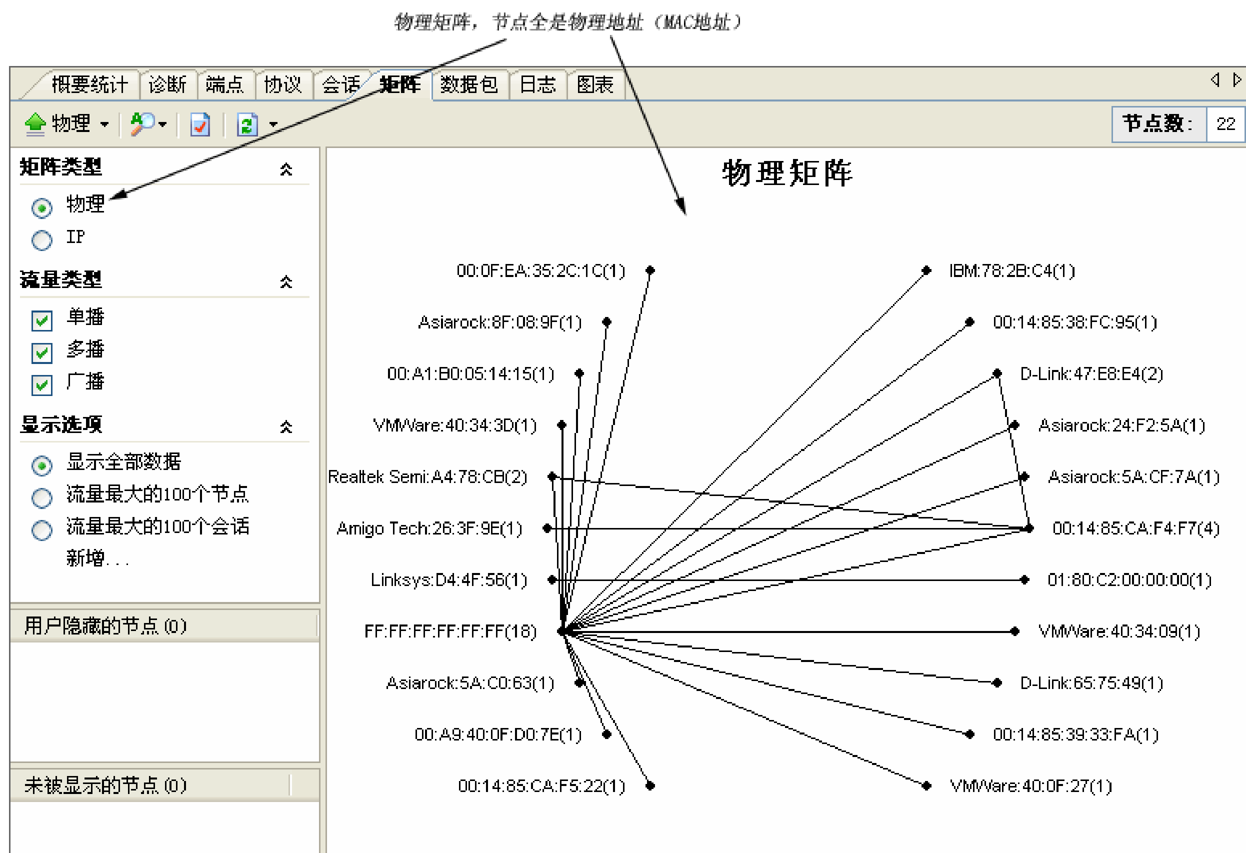


用户隐藏的节点：显示用户手动隐藏的节点信息。

未被显示的节点：显示由于应用显示过滤，而没有在矩阵内容显示区里显示的节点信息。

1． 物理矩阵

物理矩阵根据物理地址（MAC 地址）节点显示矩阵内容，界面如下图。

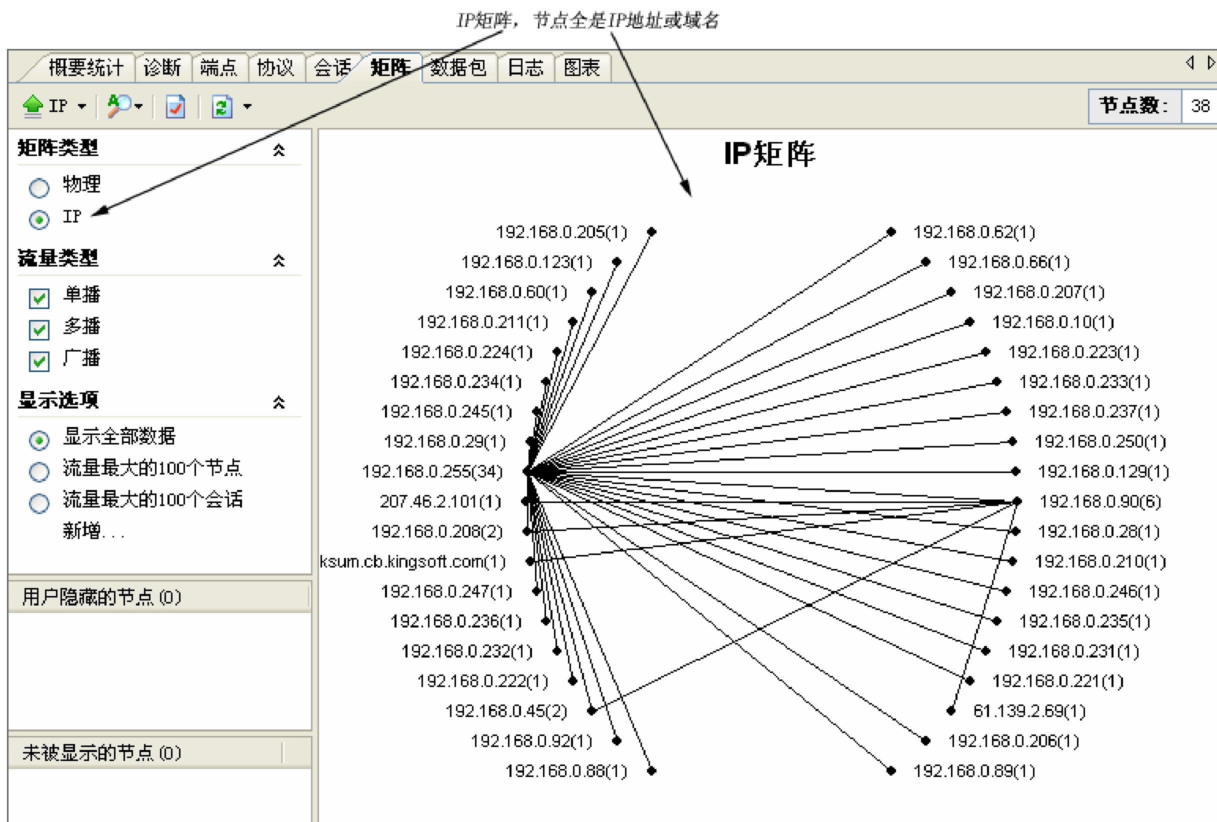


图中，由于矩阵类型选择的是物理，所以矩阵中的节点全是物理地址节点，即显示的是网卡之间的通讯。

这时，隐藏的节点和未被显示的节点中的节点信息（如果有）也是物理地址。

2. IP矩阵

IP 矩阵根据 IP 地址节点显示矩阵内容，界面如下图。



图中，由于矩阵类型选择的是 IP，所以矩阵中的节点全是 IP 地址节点，即显示的是 IP 地址之间的通讯。

这时，隐藏的节点和未被显示的节点中的节点信息（如果有）也是 IP 地址。

十四.图表

图表功能是科来网络分析系统 6.4 的一大功能，让统计分析数据表现得更为直观易读，并且提供了折线图、柱状图、面积图、饼图等多种形式，可以很方便的展现网络数据走势，也可以对比显示比例。

与其它同类软件相比，科来网络分析系统 6.4 不仅可以提供整个网络的各种统计图表，也能提供某个组，甚至是某个节点（IP、MAC、协议）的详细统计图表，让管理者对网络的应用分析管理可以大到整个网络，小到每台主机，网络的分析可以更清晰。

针对节点性质的不同，图表功能为不同的网络节点提供了多种数据类型的统计：

图表	描述
错误数据包	包括：物理错误包的统计信息、802.3 错误包的统计信息、以及错误包与正常包的对比信息。通过这些信息，我们可以确定网络的工作状态是否合理、网络的链路层是否存在故障、网络的传输是否存在故障、网络设备（如网卡）是否存在硬件错误、传输线路是否超过规定范围、网络对端设备的速率是否匹配、线路干扰是否过大等情况。
常规	对网络整体或用户选定节点的常规信息进行统计并以图表显示，包括：网络利用率、数据包数量、数据包大小分布等情况。

通过这些信息，我们可以确定网络或用户选定节点的主机的工作状态是否过于繁忙、网络中是否可能存在网络攻击、网络中数据包的增长趋势图等情况。

TCP 分析 对网络中的 TCP 连接进行统计并以图表方式显示，包括：TCP 连接、TCP 数据包、TCP 同步包、结束包和复位包等信息。

通过这些信息，我们可以确定网络内 TCP 数据包的传输质量、网络中是否存在自动运行的重传攻击、是否存在端口扫描攻击等信息。

邮件分析 对网络中的邮件收发信息进行统计并以图表方式显示。

通过此表，我们可以确定网络中发送与接收邮件的数量、比例，并帮助用户判断网络中是否有被邮件病毒感染并发起邮件蠕虫病毒攻击的主机。

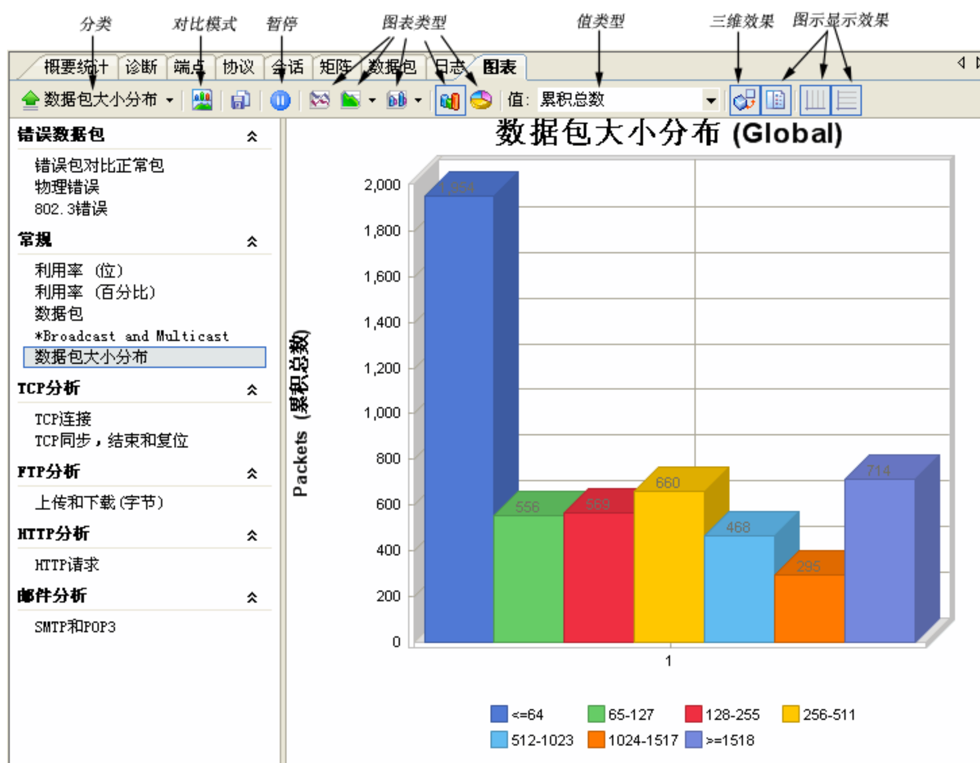
FTP 分析 对网络中的 FTP 数据传输信息进行统计并以图表方式显示。

通过此表，我们可以确定网络中通过 FTP 进行上传或下载的文件的数量、比例，并帮助用户判断网络中的 FTP 上传下载是否正常。

HTTP 分析 对网络中的 HTTP 网页访问信息进行统计并以图表方式显示。

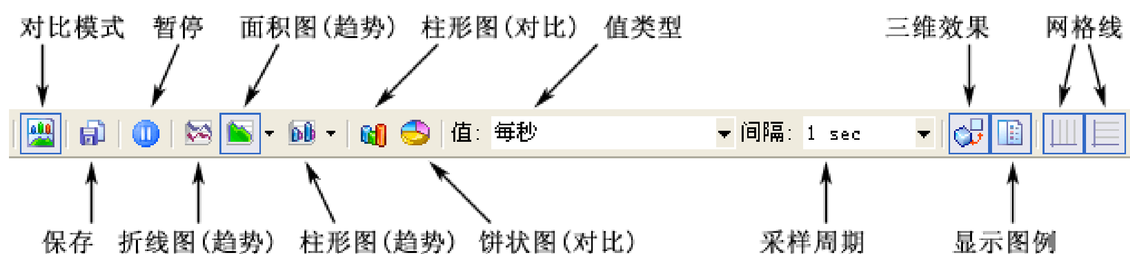
通过此表，我们可以确定网络中 HTTP 请求（网页访问）的数量、增长趋势，并帮助用户判断网络中的网页访问是否正常。

除了了解图表的数据类型，我们还应该了解一下图表选项和对比模式。



1. 图表选项

图表作为视图，也自己的视图工具栏，用户可以根据数据的类型选择不同的查看方式，如查看数据趋势，可以选择线型图，面积图，柱形图；查看数据对比，可选择柱状图对比，饼形图对比。如下图所示：



	图表类型	图表选项	操作值	采样选项
趋势图	折线图		累积总数 每秒 每次间隔值	1 秒; 5 秒; 30 秒; 60 秒; 120 秒; 300 秒; 600 秒; 3600 秒
	面积图	堆积面积图 100%堆积面积图 群组面积图	累积总数 每秒 每次间隔值	1 秒; 5 秒; 30 秒; 60 秒; 120 秒; 300 秒; 600 秒; 3600 秒
	柱形图	簇状柱形图 堆积柱形图 100%堆积柱形图 群组柱形图	累积总数 每秒 每次间隔值	1 秒; 5 秒; 30 秒; 60 秒; 120 秒; 300 秒; 600 秒; 3600 秒
对比	柱状对比		累积总数 平均每秒 最后 1 秒; 最后 5 seconds; 最后 30 秒; 最后 60 秒; 最后 120 秒; 最后 300 秒; 最后 600 秒; 最后 3600 秒	
	饼状对比		累积总数 平均每秒 最后 1 秒; 最后 5 秒; 最后 30 秒; 最后 60 秒; 最后 120 秒; 最后 300 秒; 最后 600 秒; 最后 3600 秒	

其中，面积图可提供以下三种表现形式：

堆积面积图 -- 以面积图表示，显示每一数值所占大小随时间或类别而变化的趋势线；

100%堆积面积图 -- 以面积图表示，显示每一数值所占百分比随时间或类别而变化的趋势线；

群组面积图 -- 以面积图表示，比较相交于类别轴和相交于系列轴的数值。

柱形图提供四种表现形式：

簇状柱形图 -- 以柱形图表示，比较相交于类别轴上的数值大小；

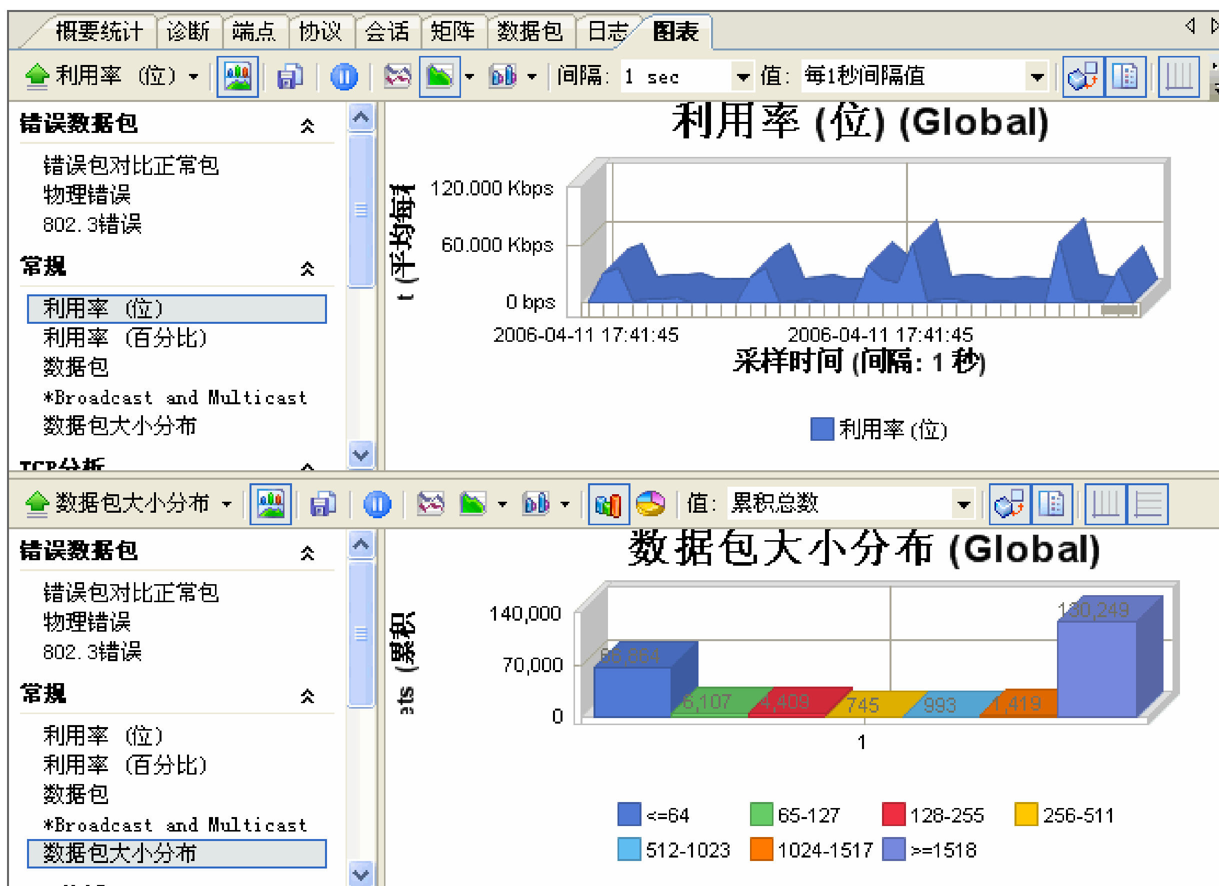
堆积柱形图 -- 以柱形图表示，比较相交于类别轴上的每一数值所占总数值的大小；

100%堆积柱形图 -- 以柱形图表示，比较相交于类别轴上的每一数值所占总数值的百分比大小；

群组柱形图 -- 以柱形图表示，比较相交于类别轴和相交于系列轴的数值。

2. 图表对比

图表查看提供数据对比模式，即对某个节点进行查看时，共同显示不同的统计数据。如下图所示，点击对比模式图标，图表视图将提供上下两个图框，管理人员可以分别选择不同的数据图表进行对比查看。再次点击对比模式图标，则会关闭对比模式。

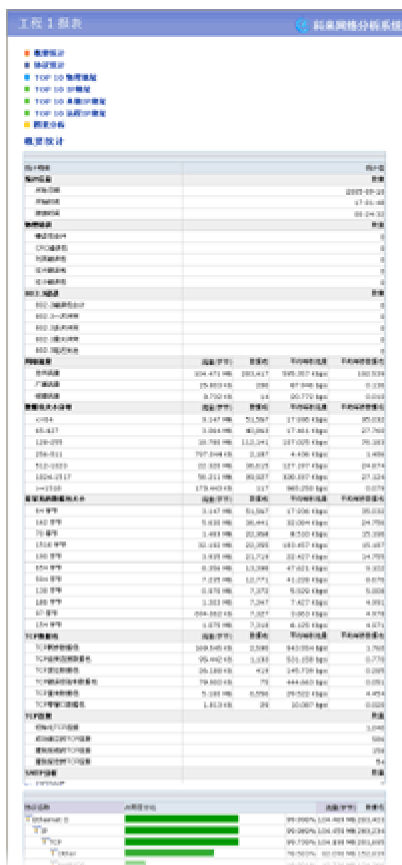


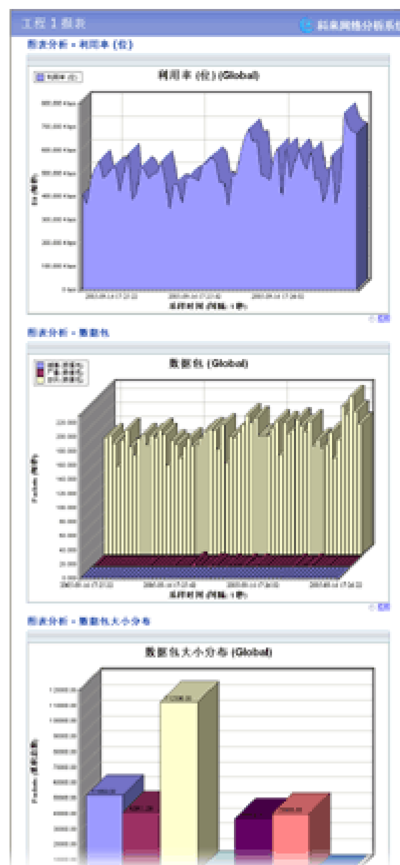
十五. 报表

报表功能可以让用户随时将统计的分析结果以报表的形式输出。用户根据报表的数据便可对当前的网络情况有一个全面的掌握。

报表包含了统计分析的主要内容，包括概要统计的全部内容、协议使用统计明细、流量最大的前 10 个 IP 地址、前 10 个 MAC 地址以及各种图形统计结果。

报表以 HTTP 格式保存在硬盘中，用户可待定保存位置，并以 IE 浏览器来打开。如果保存的路径和文件名相同，新生成的报表会更新旧报表的内容。





十六. 日志

日志视图记录网络中用户的高级网络运用，包括 HTTP 请求（网页浏览），邮件信息（通过 SMTP/POP3 进行的邮件收发）、FTP 传输（通过 FTP 进行的数据上传下载） 和 DNS 分析（域名解析），并可根据用户的需要将这些日志信息保存到硬盘以备查阅。

日志视图的界面如下图所示 （当前选定的日志类型是 HTTP 请求）。

从上图中，可以看到日志分为 4 种类型：

日志	描述
HTTP 请求	每条日志均表示由用户发起的一个 HTTP 请求，对于日志信息，系统可以捕获并统计出其对应的客户端地址、服务端地址、请求网址、请求方法、服务器响应、服务器返回的状态码、以及这条日志所持续的时间等信息。通过这些信息，我们可以有效查看网络中所有用户或者指定某用户的网页浏览情况（包括请求/被请求的网址信息，以及访问的频率），从而确定网络中是否存在恶意网页访问（攻击 Web 服务器 80 端口）、以及 Web 服务器的工作状态是否正常。
邮件信息	每条日志均表示用户通过 SMTP/POP3 协议成功进行的邮件收发操作，对于每条日志信息，可以捕获并统计出其对应客户端地址、服务端地址、邮件发送者及其邮件地址、邮件接收者及其邮件地址、邮件抄送者、邮件客户端软件、邮件内容的大小、邮件是否携带附件、以及这条日志对应操作的精确时间。通过这些信息，我们可以有效查看网络中所有用户或指定用户的邮件收发情况，从而确定网络中的邮件收发是否正常、是否存在邮件蠕虫病毒攻击、是否存在对邮件服务器的攻击等情况。
FTP	每条日志均表示用户从 FTP 服务器上传/下载一个文件的操作。对于每条日志信息，可以捕获并

传输	统计出其对应客户端地址、服务器端地址、帐号信息、操作类型（上传或下载)、传输模式（主动或被动)、传输的总字节数和总包数等信息。通过这些信息，我们可以有效查看网络中的 FTP 文件传输情况，从而确定网络中的 FTP 传输是否正常、网络中是否存在 FTP 攻击（攻击相应主机后通过 FTP 方式对其进行上传下载文件的操作）等情况。
DNS 分析	每条日志均表示服务器端返回的一个 DNS 响应。对于每条日志信息，可以捕获并统计出其对应客户端地址、客户端端口、服务器端地址、服务器端端口、查询的域名、请求是否成功、服务器端的回答、权威回答、附加效果、以及具体的分析结果。通过这些信息，可以有效查看网络中所有用户或特定用户的 DNS 请求及响应情况。

1. HTTP请求日志

在 HTTP 请求日志中，每条日志均表示由用户发起的一个 HTTP 请求，对于日志信息，系统可以捕获并统计出其对应的客户端地址、服务端地址、请求网址、请求方法、服务器响应、服务器返回的状态码、以及这条日志所持续的时间等信息。通过这些信息，我们可以有效查看网络中所有用户或者指定某用户的网页浏览情况（包括请求/被请求的网址信息，以及访问的频率），从而确定网络中是否存在恶意网页访问（攻击 Web 服务器 80 端口）、以及 Web 服务器的工作状态是否正常。

HTTP 请求日志的界面如下图所示。

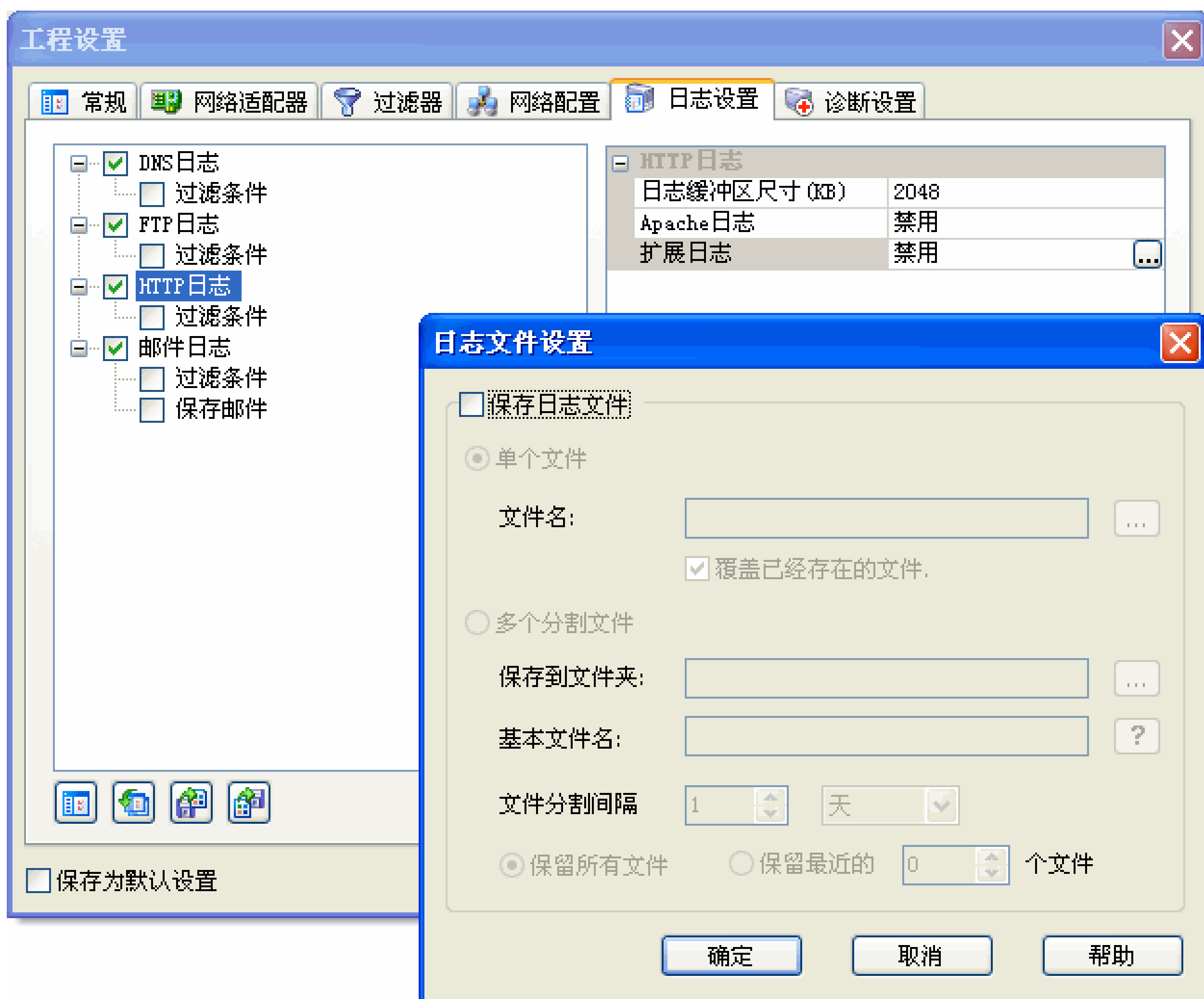
概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

HTTP请求　　日志: 41

日志: HTTP请求 / 邮件信息 / FTP传输 / DNS分析

时间	客户端	服务端	请求网址	请求方法	状态码
09:29:26	192.168.0.90:1551	tools.l.google.com:www-http	http://toolbar.google.com/...	GET	302
09:29:26	192.168.0.90:1552	www-china.l.google.com:www...	http://www.google.com/tool...	GET	200
09:29:45	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn/	GET	200
09:29:46	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:47	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:47	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:50	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:51	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:52	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:53	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:55	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1559	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:56	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304
09:29:57	192.168.0.90:1558	www.colasoft.com.cn:www-http	http://www.colasoft.com.cn...	GET	304

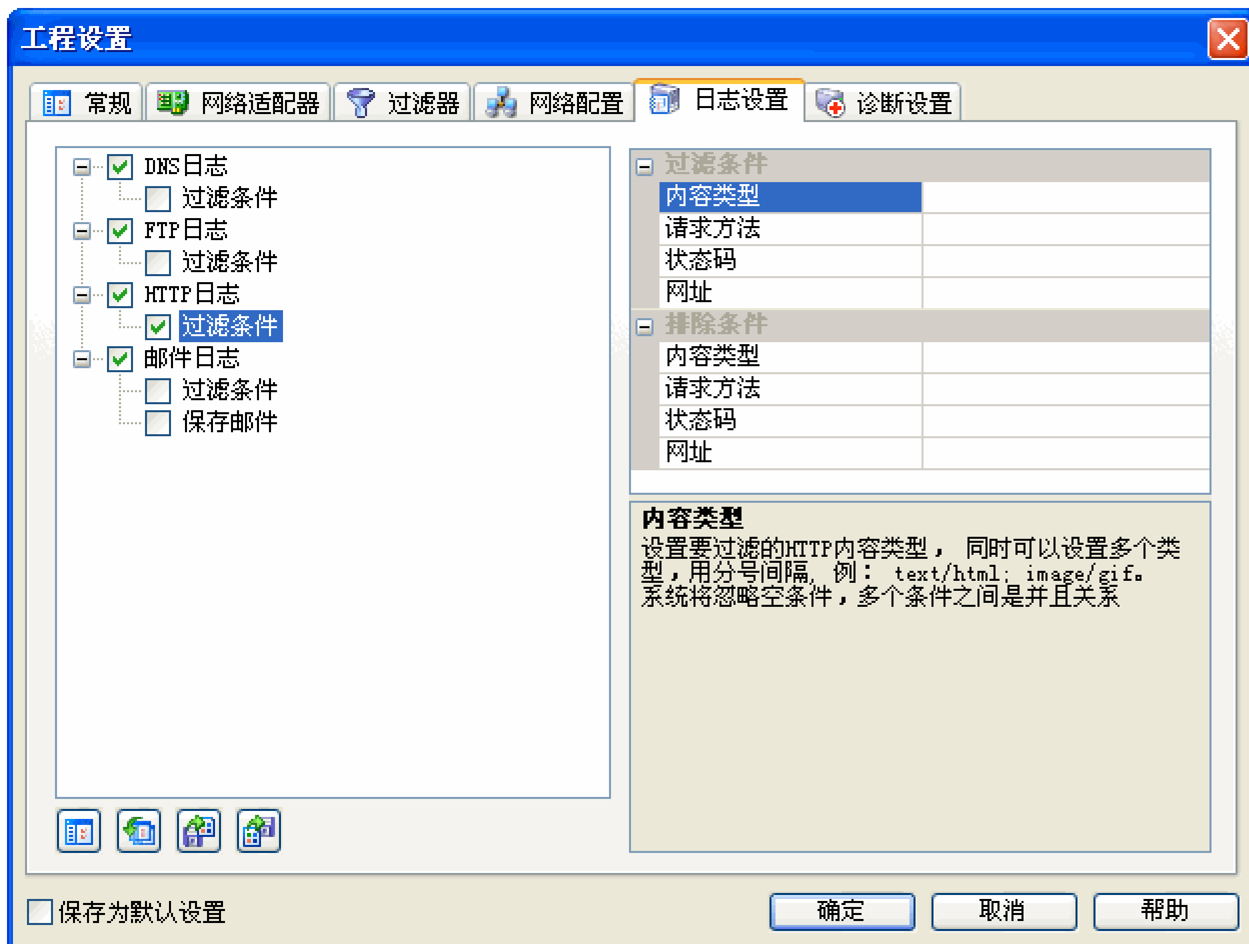
用户还可以在“工程设置->日志设置”中修改日志缓冲区大小及自定义保存日志，如下图所示。



系统默认缓冲区大小为 2048KB。

日志文件可以保存为单个文件，也可以按照日期或文件大小来分割成单独的文件，同时也可定义日志保存的数量，使日志文件不会无限增加。

用户还可以在日志设置中添加 HTTP 日志过滤条件，系统默认没有启用，如下图所示。



用户可以在设置内容类型、请求方法、状态码、网址 4 种过滤条件。

2. 邮件信息日志

在邮件信息中，每条日志均表示用户通过 SMTP/POP3 协议成功进行的邮件收发操作，对于每条日志信息，可以捕获并统计出其对应客户端地址、服务端地址、邮件发送者及其邮件地址、邮件接收者及其邮件地址、邮件抄送者、邮件客户端软件、邮件内容的大小、邮件是否携带附件、以及这条日志对应操作的精确时间。通过这些信息，我们可以有效查看网络中所有用户或指定用户的邮件收发情况，从而确定网络中的邮件收发是否正常、是否存在邮件蠕虫病毒攻击、是否存在对邮件服务器的攻击等情况。

邮件信息日志的界面如下图所示。

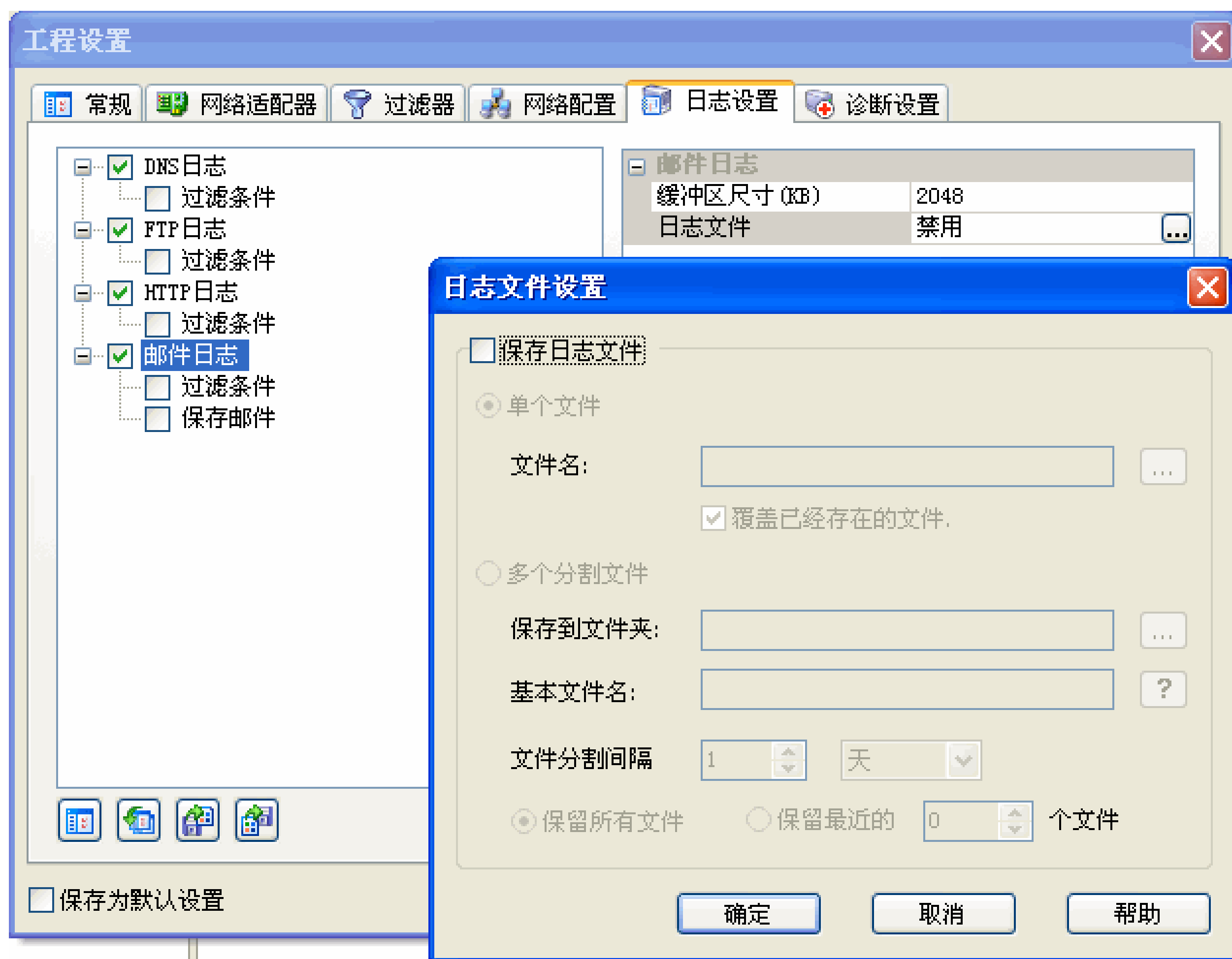
概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表 报表

邮件信息 日志: 7

日志: HTTP请求 邮件信息 FTP传输 DNS查询

日期	时间	客户端	服务端	发送者	发送邮件地址
2006-11-17	09:43:42	192.168.0.92:1353	220.181.12.101:110	拍拍乐影像家园	mailer@pixplayer.com
2006-11-17	09:43:43	192.168.0.92:1353	220.181.12.101:110	javadaiy	javadaiy@126.com
2006-11-17	09:45:17	192.168.0.92:1353	220.181.12.101:110	优点yodian.com	ad148@m349.yodian.com.cn
2006-11-17	09:45:19	192.168.0.92:1353	220.181.12.101:110		info@testkingmail.com
2006-11-17	09:45:20	192.168.0.92:1353	220.181.12.101:110	NetBuddy.Org成员	xxbin@netbuddy.org
2006-11-17	09:45:20	192.168.0.92:1353	220.181.12.101:110		support@bokee.com
2006-11-17	09:45:21	192.168.0.92:1353	220.181.12.101:110	西陆网(www.xilu...	admin@xilu.com

用户还可以通过“工程设置->日志设置”中修改缓冲区大小及自定义保存日志文件。如下图所示。

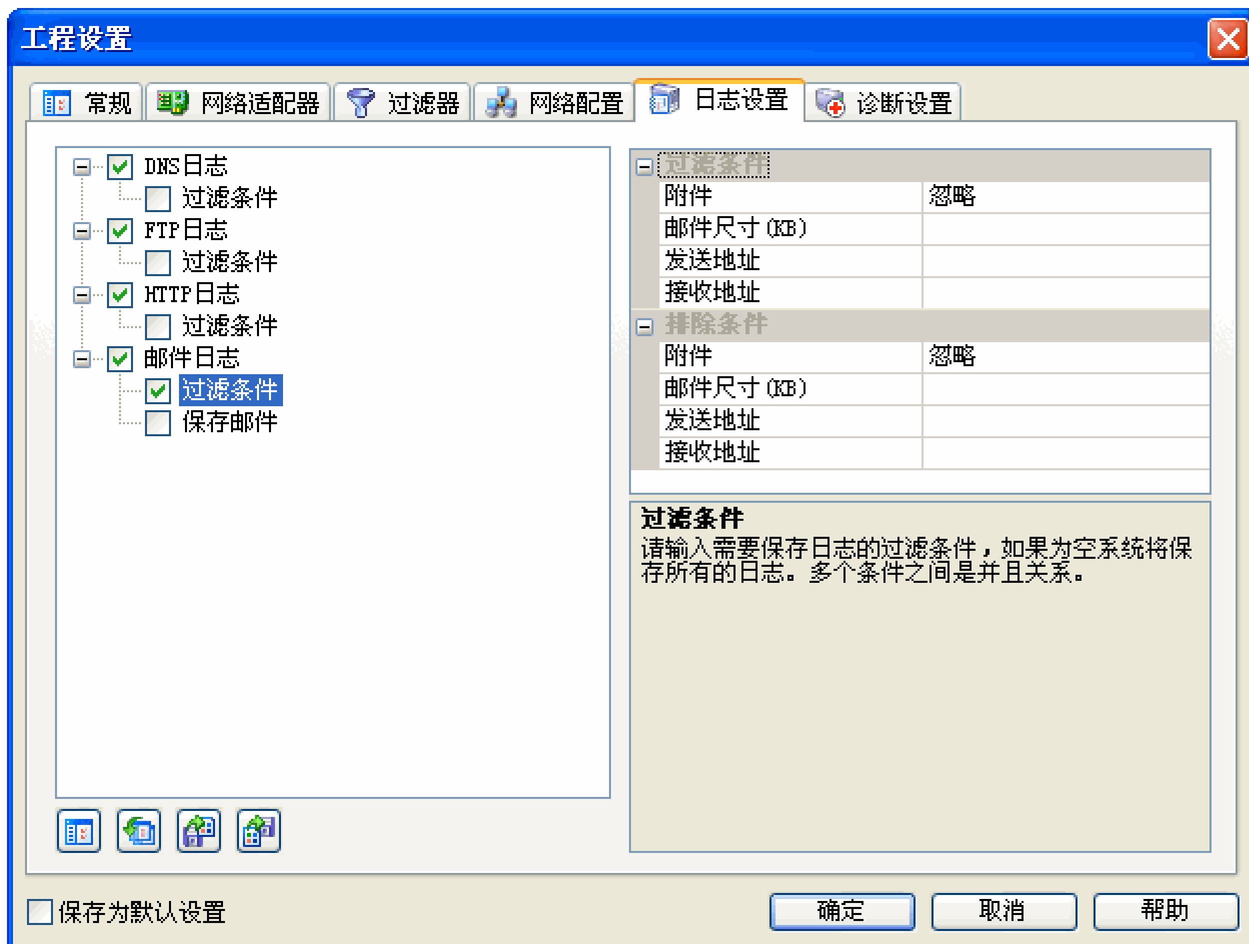


系统默认缓冲区大小为 2048KB。

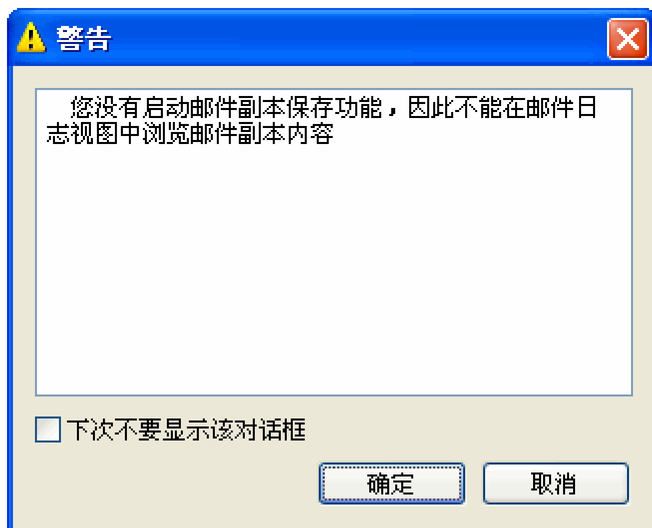
日志文件可以保存为单个文件，也可以按照日期或文件大小来分割成单独的文件，同时也可定义日志保存的数量，使日志文件不会无限增加。

用户还可以在日志设置中设置过滤条件和保存邮件副本。

过滤条件包括：是否忽略附件、邮件尺寸、发送地址、接收地址的设置。系统默认没有启用。如下图所示。



用户还可以将邮件副本保存到硬盘，以备以后查阅。系统默认没有启用，所以在开始捕获数据时也会弹出警告信息。如下图。



3. FTP传输日志

在 FTP 传输中，每条日志均表示用户从 FTP 服务器上传/下载一个文件的操作。对于每条日志信息，可以捕获并统计出其对应客户端地址、服务器端地址、帐号信息、操作类型（上传或下载）、传输模式（主动或被动）、传输的总字节数和总包数等信息。通过这些信息，我们可以有效查看网络中的 FTP 文件传

输情况，从而确定网络中的 FTP 传输是否正常、网络中是否存在 FTP 攻击（攻击相应主机后通过 FTP 方式对其进行上传下载文件的操作）等情况。

FTP 传输日志的界面如下图所示。

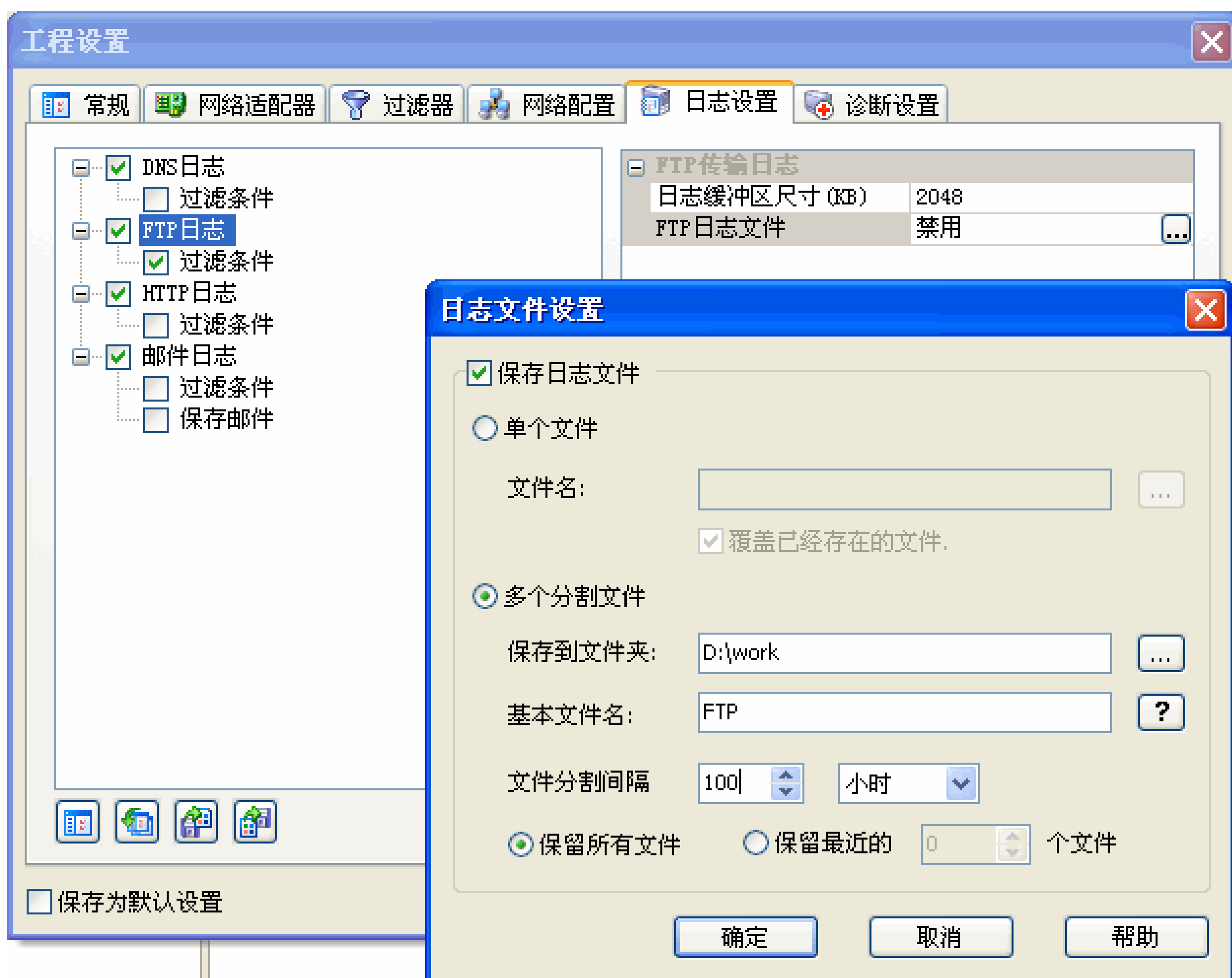
概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

FTP传输 日志: 28

日志: HTTP请求, 邮件信息, FTP传输, DNS查询

序号	客户端	服务端	帐号	操作类型	路径	传输模式	总字节数
1	192.168.0.92:2321	192.168.0.90:2996	wangyiming	RETR	IPv6_ip.pdf	PASV	2483097
2	192.168.0.92:2332	192.168.0.90:3007	wangyiming	RETR	spantree.swf	PASV	84912
3	192.168.0.92:2333	192.168.0.90:3008	wangyiming	RETR	URL编码.xls	PASV	21504
4	192.168.0.92:2334	192.168.0.90:3009	wangyiming	RETR	对称协议和非...	PASV	203
5	192.168.0.92:2346	192.168.0.90:3013	wangyiming	STOR	chs_beta_sn.txt	PASV	8333
6	192.168.0.92:2348	192.168.0.90:3015	wangyiming	STOR	capsa.xml	PASV	11995
7	192.168.0.92:2349	192.168.0.90:3016	wangyiming	STOR	capsa_pro.xml	PASV	11435
8	192.168.0.92:2350	192.168.0.90:3017	wangyiming	STOR	chs_beta_sn.txt	PASV	8333
9	192.168.0.92:2351	192.168.0.90:3018	wangyiming	STOR	CMM2.0Beta20...	PASV	31744
10	192.168.0.92:2352	192.168.0.90:3019	wangyiming	STOR	DNS服务器.txt	PASV	1357
11	192.168.0.92:2353	192.168.0.90:3020	wangyiming	STOR	IPv6_ip.pdf	PASV	2483097
12	192.168.0.92:2354	192.168.0.90:3021	wangyiming	STOR	MSN_monitor1...	PASV	105984
13	192.168.0.92:2355	192.168.0.90:3022	wangyiming	STOR	NOiE.cap	PASV	25573
14	192.168.0.92:2356	192.168.0.90:3023	wangyiming	STOR	spantree.swf	PASV	84912
15	192.168.0.92:2357	192.168.0.90:3024	wangyiming	STOR	Thumbs.db	PASV	4608
16	192.168.0.92:2358	192.168.0.90:3025	wangyiming	STOR	URL编码.xls	PASV	21504
17	192.168.0.92:2359	192.168.0.90:3026	wangyiming	STOR	wan1.doc	PASV	27648
18	192.168.0.92:2360	192.168.0.90:3027	wangyiming	STOR	~$应用范例.doc	PASV	162
19	192.168.0.92:2361	192.168.0.90:3028	wangyiming	STOR	~WRL0079.tmp	PASV	135680
20	192.168.0.92:2363	192.168.0.90:3031	wangyiming	RETR	DNS服务器.txt	PASV	1357

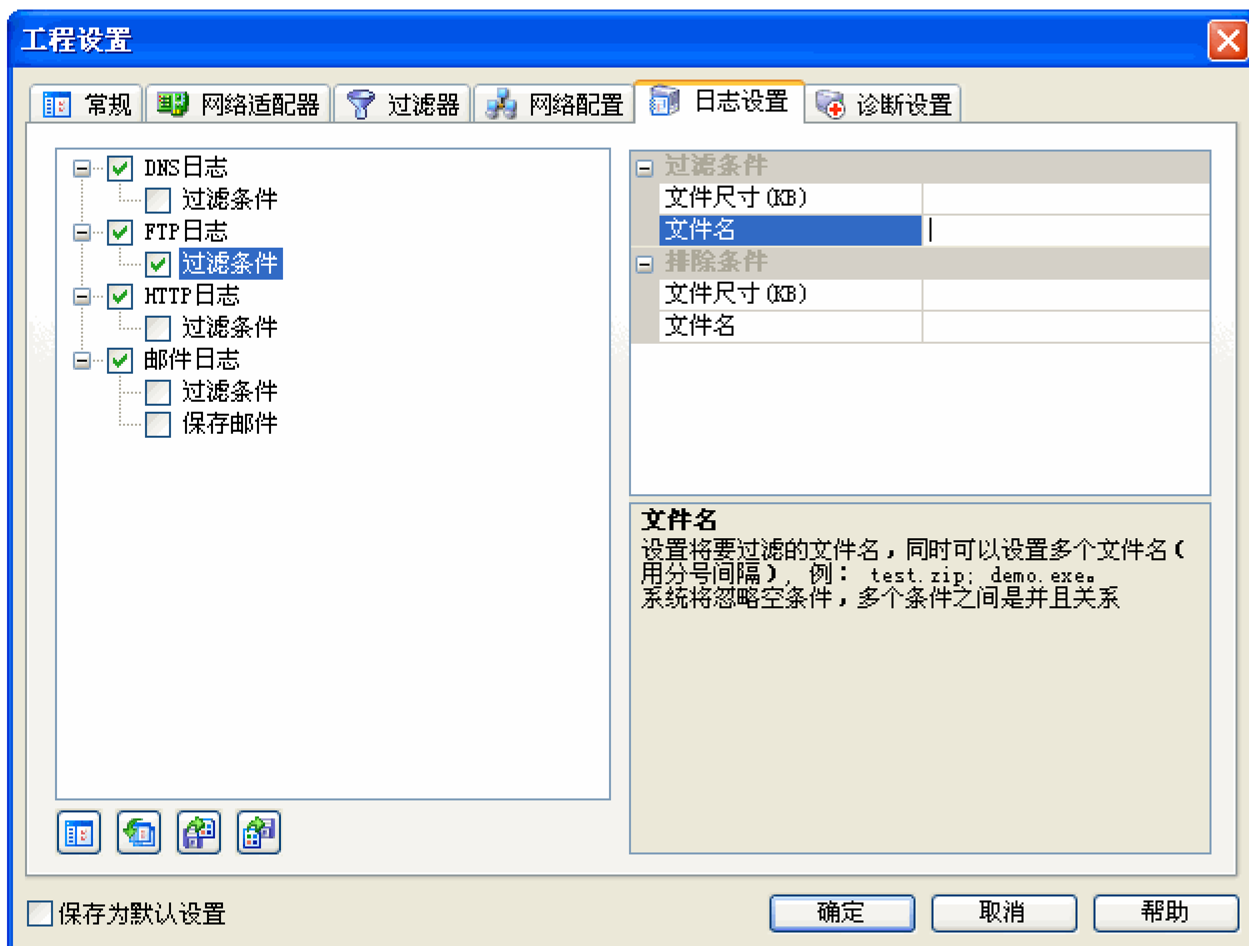
用户还可以在“工程设置->日志设置”中修改日志缓冲区大小及自定义保存日志，如下图所示。



系统默认缓冲区大小为 2048KB。

日志文件可以保存为单个文件，也可以按照日期或文件大小来分割成单独的文件，同时也可定义日志保存的数量，使日志文件不会无限增加。

用户还可以设置 FTP 日志过滤条件，系统默认没有启用。如下图所示。



用户可以在根据文件尺寸及文件名来设置过滤器条件。

4. DNS传输日志

在 DNS 查询日志中，显示网络中 FTP 传输数据包的统计信息，包括 FTP 控制连接数、登录失败次数、成功的数据连接数、以及访问的服务器数等。通过这些信息，我们可以确定网络中进行 FTP 数据上传下载的情况，包括 FTP 服务器的数据是否被未被允许的上传下载，网络中是否存在 FTP 账户的用户名密码的情况，以及对上传下载的数据进行统计。

DNS 查询日志的界面如下图所示。

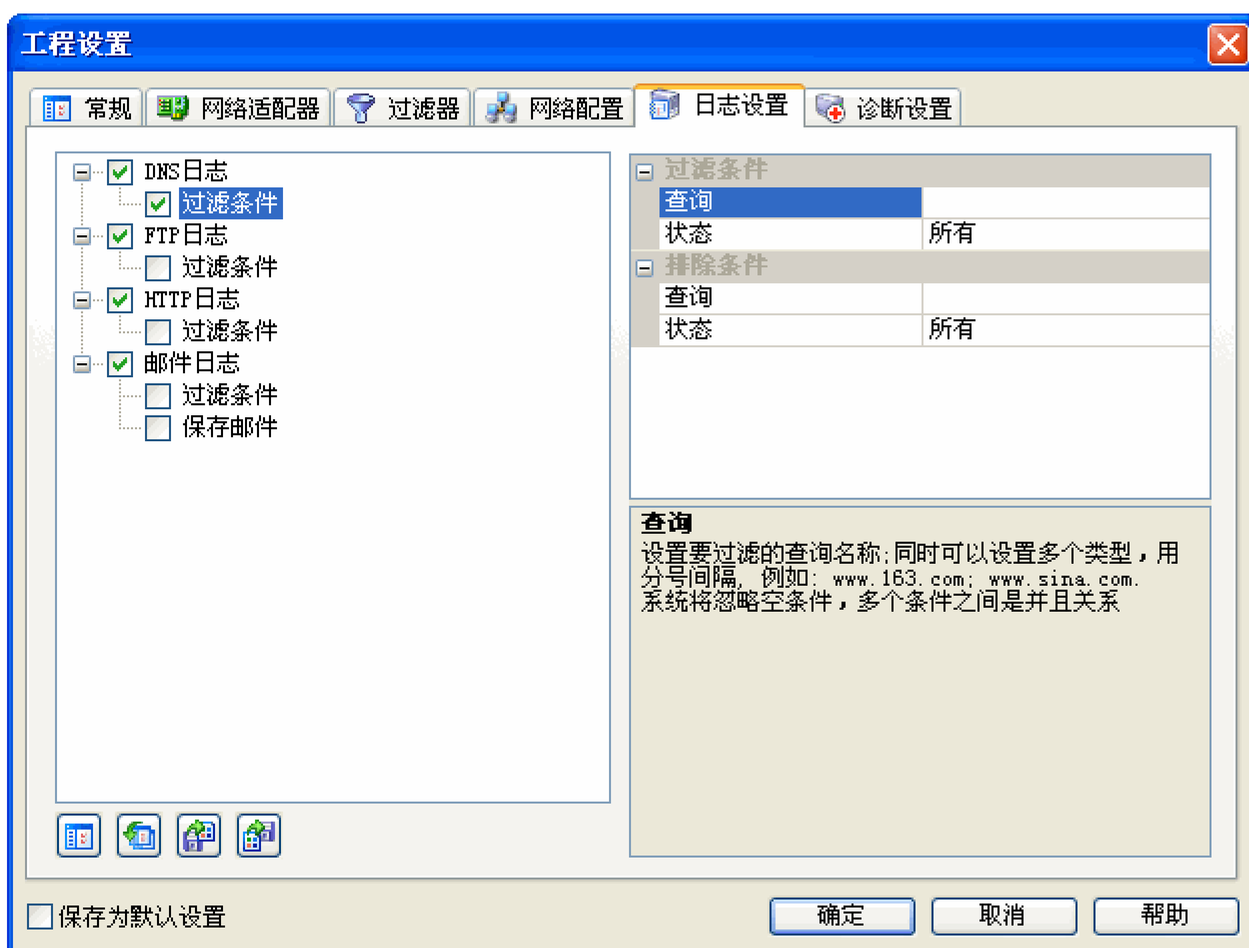
概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表 报表

DNS查询 日志: 14

日志: HTTP请求 邮件信息 FTP传输 DNS查询

时间	客户端	服务器端	查询	状态	分析结果
09:31:41	192.168.0.92:1026	192.168.0.1:53	www.baidu.com	成功	CNAME=www.a.shifen.com; A=220.181.18...
09:31:41	192.168.0.92:1026	192.168.0.1:53	c.baidu.com	成功	CNAME=c.a.shifen.com; A=220.181.18.186
09:31:44	192.168.0.92:1026	192.168.0.1:53	www.onlinedown.net	成功	A=61.232.206.210; A=61.232.206.243; ...
09:31:46	192.168.0.92:1026	192.168.0.1:53	qa.qicaihong.com	成功	A=61.142.80.227
09:31:46	192.168.0.92:1026	192.168.0.1:53	pdlib.pconline.com.cn	成功	CNAME=pdlib.pconline.chinacache.net;...
09:31:51	192.168.0.92:1026	192.168.0.1:53	www.newhua.com	成功	A=61.232.206.210; A=61.232.206.243; ...
09:31:55	192.168.0.92:1026	192.168.0.1:53	pagead2.googlesyndic...	成功	CNAME=pagead2.google.com; CNAME=page...
09:32:01	192.168.0.92:1026	192.168.0.1:53	union.3721.com	成功	A=202.165.102.145; A=202.165.102.143...
09:32:01	192.168.0.92:1026	192.168.0.1:53	www.donews.com	成功	A=211.100.32.252
09:32:09	192.168.0.92:1026	192.168.0.1:53	admin.onlinedown.net	成功	A=218.93.205.61
09:32:13	192.168.0.92:1026	192.168.0.1:53	cookie.onlinedown.net	成功	A=61.234.56.154; A=211.98.38.4; A=21...
09:33:02	192.168.0.92:1026	192.168.0.1:53	s.baidu.com	成功	CNAME=s.a.shifen.com; A=220.181.18.124
09:33:15	192.168.0.92:1026	192.168.0.1:53	s59.cnzz.com	成功	A=222.77.187.23
09:33:47	192.168.0.92:1026	192.168.0.1:53	wpa.qq.com	成功	A=219.133.49.158; A=219.133.38.16; A...

用户还可以在 “ 工程设置->日志设置 ” 中设置缓冲区大小及日志过滤条件，设置界面如下图。



系统默认缓冲区大小为 2048KB。

系统默认没有启用过滤条件，若启用该功能，用户可以设置查询及状态。

十七.数据包解码

科来网络分析系统 6.4 通过解码器，对捕获到的数据包进行自动解码。解码是对数据包的每层信息进行详细解释和分析，达到网络最细化的分析。

网络分析越细化，也意味着网络的管理者可以更加容易地发现网络中存在的异常情况；采集更为精确的数据样本，并进行诊断和分析，以便及时制定应对策略。同时，数据包解码分析可极大提升网络应用辨别能力，也让用户可以迅速找出那些可能会降低网络性能 或网络攻击的潜在因素。

与此同时，“高清晰的数据包分析”功能也很好的弥补了现有网络管理系统的不足。因为在当今网络中数据传输种类不断增加、网络流量不断加快、网络结构日益复杂的情况下，网络中的异常情况很可能是稍纵即逝的，通过传统的网络管理手段很难做到对网络故障、网络攻击进行精确地定位、捕捉和分析。但是通过“高清晰 的数据包分析”，网络的管理者可以通过信息包的捕获查看每个数据包的内容，能清楚地了解应用的来源，目的，作用以及其他细节，从而在庞杂的数据流中找出那些可能存在的问题。

数据包解码由概要解码、字段解码、十六进制解码组成，由三个视图框组成，用户可以改变解码视图框的排列方式和组合方式。

概要显示视图逐行显示捕获到的数据包概要信息

(-) 表示在多行显示解码信息
(+) 表示在一行显示解码信息

字段解码视图框显示所选数据包字段的详细信息

十六进制解码

ASCII或EBCDIC解码

通过解码，我们可以了解以下信息：

数据包的概要信息（作用、以及提取的重要值）；

网络中的数据包的类型；

网络中传输的数据包是否正确；

网络中 IP 数据包的版本；

目标主机是否在运行客户端主机所请求的服务；

源主机到目标主机间的路由时间（即链路长度）；

目标主机对客户端主机请求的服务的响应时间；

网络中传输的数据是否为紧急数据；

数据包在网络中经过的路由跳数；

网络中是否存在环路现象；

用户访问目标主机某服务的原始步骤；

1. 概要解码

概要解码逐行显示每一个捕获数据包的概要信息。

概要信息主要包括：数据包被捕获的绝对时间、源 IP 及使用端口、发送的目标 IP 及端口、使用的协议、数据包的大小、概要内容等。

对数据包进行查看，管理人员可以：

设定显示选项，自定义要查看的数据列

双击打开新窗口查看数据包解码的全部内容

高亮显示选择的数据包

对感兴趣的数据包添加注释

选择相关联的数据包

通过 Page UP 和 Page Down 来浏览前后数据包

通过数据包生成过滤器

导出数据包

定位该数据包所在节点

将 MAC 地址或 IP 地址添加到名字表

使用滚屏功能始终显示最新的数据包

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

数据包: 37,819

编号	绝对时间	源	目标	协议	大小	解码	概要
3301	11:48:02.088484	192.168.0.93:2028	192.168.0.208:8080	HTTP Proxy	64	003301	序列号=110709891...
3302	11:48:06.434597	192.168.0.93:1028	192.168.0.208:5001	TCP	64	003302	序列号=071601182...
3303	11:48:06.434990	192.168.0.93:1027	192.168.0.208:5001	TCP	64	003303	序列号=318523134...
3304	11:48:06.435367	192.168.0.93:1025	192.168.0.208:5001	TCP	64	003304	序列号=391558415...
3305	11:48:06.582679	192.168.0.208:5001	192.168.0.93:1027	TCP	64	003305	序列号=045896664...
3306	11:48:06.582767	192.168.0.208:5001	192.168.0.93:1028	TCP	64	003306	序列号=408571516...
3307	11:48:06.582792	192.168.0.208:5001	192.168.0.93:1025	TCP	64	003307	序列号=344141300...
3308	11:48:07.116288	192.168.0.90:137	192.168.0.255:137	NBNS	96	003308	C: 名称=WORKGROU...
3309	11:48:07.865053	192.168.0.90:137	192.168.0.255:137	NBNS	96	003309	C: 名称=WORKGROU...
3310	11:48:08.615327	192.168.0.90:137	192.168.0.255:137	NBNS	96	003310	C: 名称=WORKGROU...
3311	11:48:14.221895	192.168.0.208:137	192.168.0.255:137	NBNS	96	003311	C: 名称=OFFICE <1B>
3312	11:48:14.971227	192.168.0.208:137	192.168.0.255:137	NBNS	96	003312	C: 名称=OFFICE <1B>
3313	11:48:15.721478	192.168.0.208:137	192.168.0.255:137	NBNS	96	003313	C: 名称=OFFICE <1B>
3314	11:48:17.124552	192.168.0.208:8080	192.168.0.93:2028	HTTP Proxy	87	003314	序列号=267376239...

2. 字段解码

字段解码也称为详细解码，可以看到数据包的详细信息。默认情况下，科来网络分析系统将在字段解码框中逐层展开协议层的内容，并按照树型结构显示。要节省查看空间，请单击协议子层前面的减号(-)。要再次展开协议显示，请单击加号(+)。点鼠标右键的"复制树结构"，可以将协议子层的数据复制到剪切板上。

如果想了解字段的详细信息，可查看网站提供的常见协议详细解码资料。

概要统计 | 诊断 | 端点 | 协议 | 会话 | 矩阵 | 数据包 | 日志 | 图表 | 报表

IP\数据包: 4,852

编号	绝对时间	源	目标	协议	大小	概要
5191	09:39:14.785363	192.168.0.90:1383	192.168.0.208:5001	TCP	64	序列号=127990287...
5192	09:39:14.785480	192.168.0.90:1382	192.168.0.208:5001	TCP	64	序列号=127969288...
5194	09:39:14.982207	192.168.0.208:5001	192.168.0.90:1382	TCP	64	序列号=065835963...
5195	09:39:14.982259	192.168.0.208:5001	192.168.0.90:1383	TCP	64	序列号=316337996...
5196	09:39:14.982270	192.168.0.208:5001	192.168.0.90:1384	TCP	64	序列号=321326757...
5197	09:39:15.024419	207.46.114.54:1863	192.168.0.90:1064	MSN	205	序列号=307526949...
5198	09:39:15.136170	192.168.0.90:1064	207.46.114.54:1863	MSN	64	序列号=102981647...
5203	09:39:20.793710	192.168.0.208:138	192.168.0.255:138	NBDGM	247	C: Transaction N...

数据包: 编号:005191 长度:64 捕获长度:60 时间戳:2006-04-12 09:39:14.785363
ETH II 目标:00:E0:4C:A4:78:CB 源:00:14:85:CA:F4:F7 协议:0x0800
IP 版本:4 头长:5 DSF:0000 0000 总长:46 标识:0x6DDB 标志:010. .... 段偏移:0
TCP - 传输控制协议 [34/20] 字段的详细解码
源端口: 1383 (gwha) [34/2]
目标端口: 5001 (commplex-link) [36/2]
序列号: 1279902877 [38/4]
确认号: 3163379960 [42/4]

3. 十六进制解码

十六进制解码是以十六进制和 ASCII(或 EBCDIC)格式显示所选数据包。当您选择"概要解码"中的数据包或在"字段解码"选择了协议字段后，该数据包相应的十六进制字节(Hex 格式)将在"十六进制解码视图框"中高这显示，如图所示。这样您可以很快的了解协议字段与它在数据包中相应字节的对应关系。

字段解码视图框显示所选
数据包字段的详细信息

Packet Info:
Packet Number: 005361
Packet Length: 66
Capture Length: 62
Timestamp: 2005-09-13 17:34:24.012993
Ehternet - II Header [0/0]
Destination Address: 00:80:C8:21:64:D4 D-Link Sys [0/6]
Source Address: 00:0B:6A:5A:E8:2E Asiarock [6/6]

```
0000  00 80 C8 21 64 D4 00 0B 6A 5A E8 2E 08 00 45 00 00 30 01 14   ...!d...jZ....E..0..
0014  40 00 80 06 CA 3E C0 A8 00 42 D3 C4 9A C6 0D 8C 00 50 8F E0   @...>...B.......P..
0028  9C 3E 00 00 00 00 70 02 FA F0 1E BE 00 00 02 04 05 B4 01 01   .>....p.............
003C  04 02                                                         ..
```

对应的 Hex 格式数据　　对应的 ASCII（或EBCDIC）格式数据

十八.TCP 数据流重组

科来网络分析系统可以将捕获到的网络数据按照正确的顺序，重组成 TCP 片段。根据 TCP 数据流，管理人可以完全掌握数据的通讯情况。利用 TCP 数据流中的会话信息，可以很容易跟踪每个网络会话的整个过程，包括客户端与服务器端之间的请求与响应。

科来网络分析系统支持主要 TCP 应用的重组，包括：web(HTTP)、email(SMTP/POP3)、FTP、NBSSN、MSN 等。

下图所示，是一个 HTTP 的数据流重组结果，我们可以看到客户端与服务器端之间的会话详细过程。

概要统计 诊断 端点 协议 会话 矩阵 数据包 日志 图表 报表
TCP　会话: 2

端点1 ->	<- 端点2	包 ->	<- 包	字节 ->	<- 字节
192.168.0.90:3518	64.246.27.237:www-http	42	48	6.815 KB	57.018 KB
192.168.0.90:3519	64.246.27.237:www-http	39	44	5.899 KB	54.966 KB

会话：物理 IP TCP UDP

数据包 数据流
192.168.0.90:3518 <-> 64.246.27.237:80\数据包: 90

```
端点 1: IP地址 = 192.168.0.90, TCP端口 = 3518
端点 2: IP地址 = 64.246.27.237, TCP端口 = 80

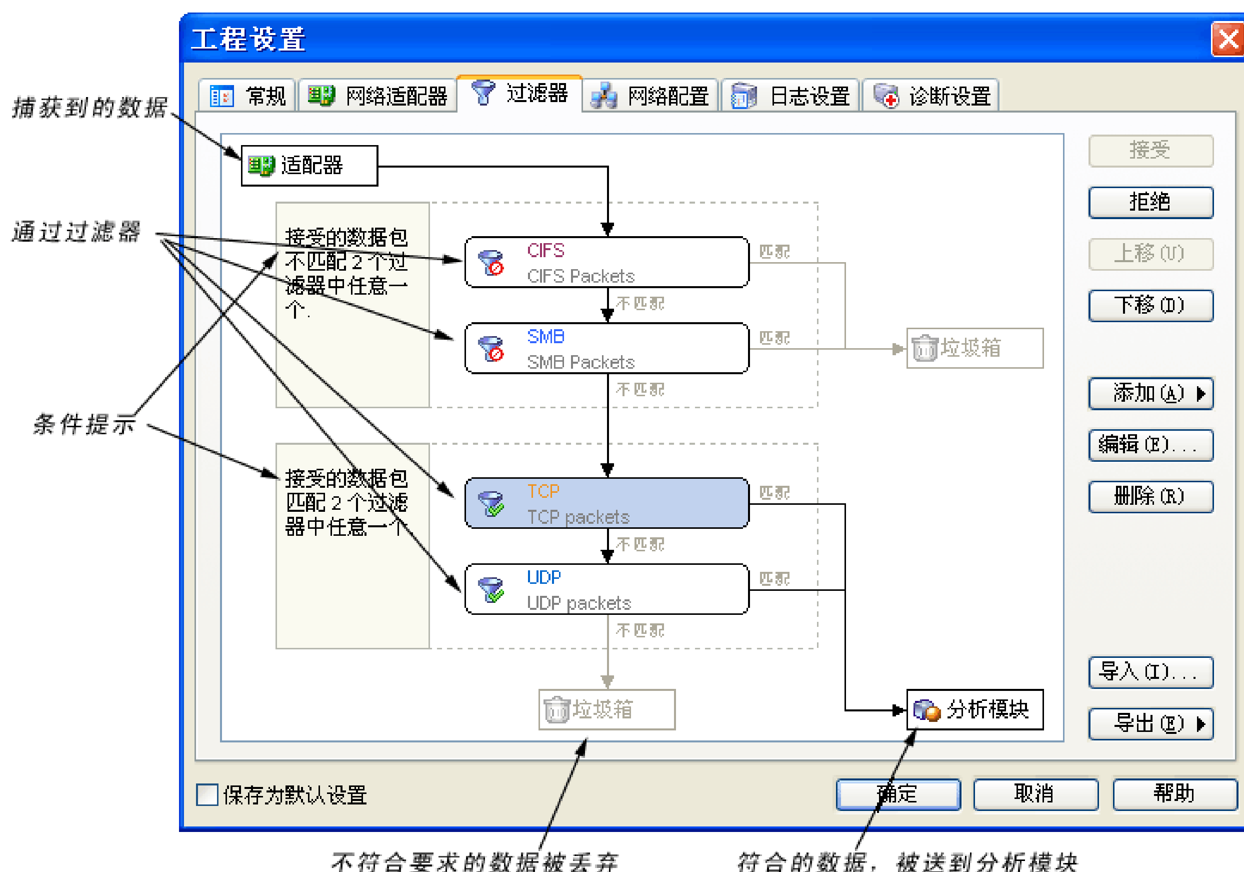
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, application/x-shockwave-
flash, */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; .NET CLR 1.1.4322)
Host: www.colasoft.com.cn
Connection: Keep-Alive
Cookie: PageNum=12; UserCookie=1143068412517
```

十九.过滤器

设置过滤器是我们改变捕获数据范围的重要手段。通过过滤器，我们可以只捕获所需的特定数据包，把重要的数据分离出来。这样，你就可以只关注存在网络故障或网络攻击的数据信息，而不用在大量的数据中逐个寻找。

用户可在工程设置中来定义过滤器设置，选择工具栏图标 则进入过滤器设置对话框。科来网络分析系统提供了一个默认的过滤器列表。这些过滤器都是以按照协议为条件的过滤器，每个过滤器都可以使用“接收”和“排除”来指定其过滤条件。也可以随意组合其中的过滤器来制定数据包的捕获范围。

如果用户感兴趣，可以设定查找病毒的过滤器，查找 BT 数据包的过滤器等。按照直观性，我们把过滤器的设置又分为“简单过滤器”和“高级过滤器”。由于高级过滤的筛选条件多于简单过滤，这样简单过滤器可以转换为高级过滤器，而高级过滤器转换为简单过滤器将会丢失一些筛选条件。

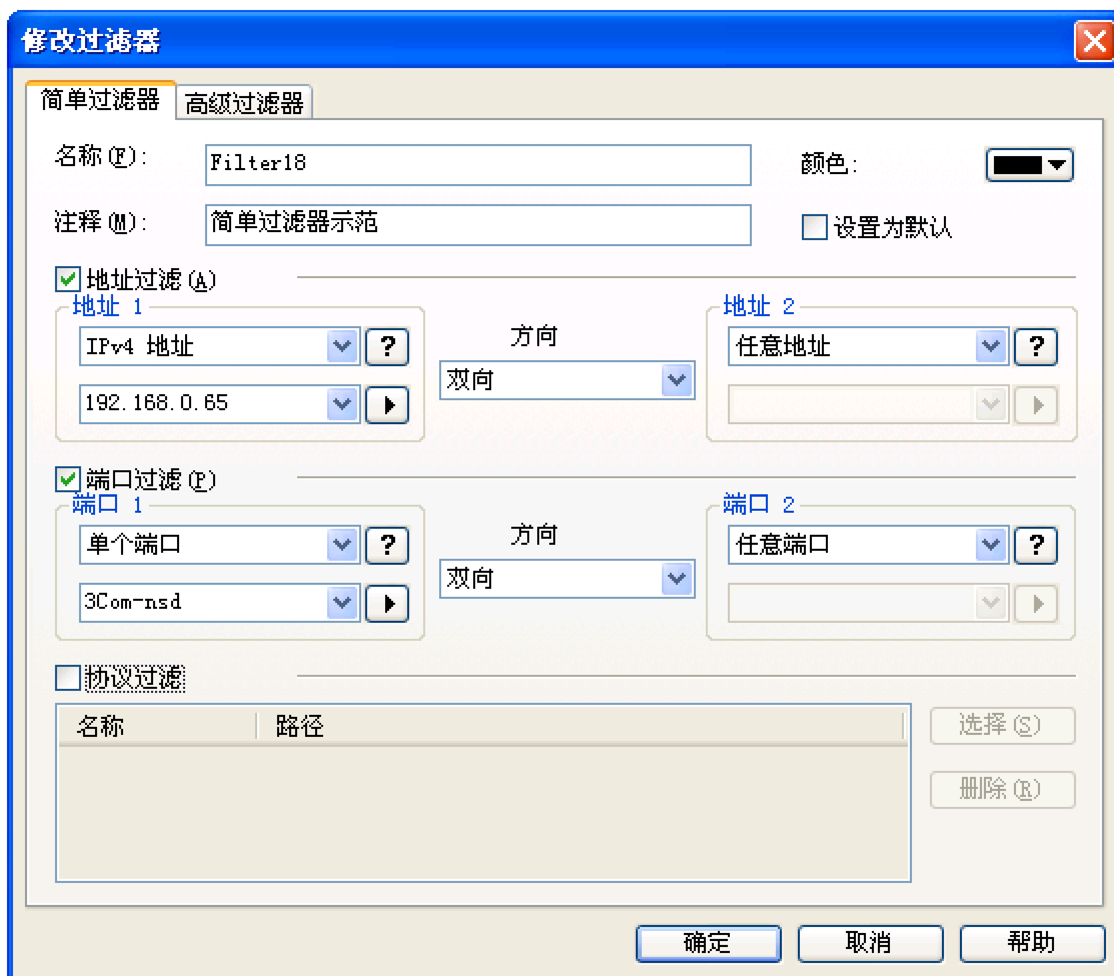


1. 简单过滤

简单过滤可以让你使用常用的筛选条件，如 IP 地址、MAC 地址、端口、协议等。

在设置 IP 地址、MAC 地址、端口这些条件时，可以选择数据包传输的方向。这样可以很精确的进行筛选数据。而设定协议条件时，可以选择一个或多个协议进行筛选。

简单过滤中的筛选条件可以任意组合，并且为了查看方便，可指定协议的颜色以区别其它协议。



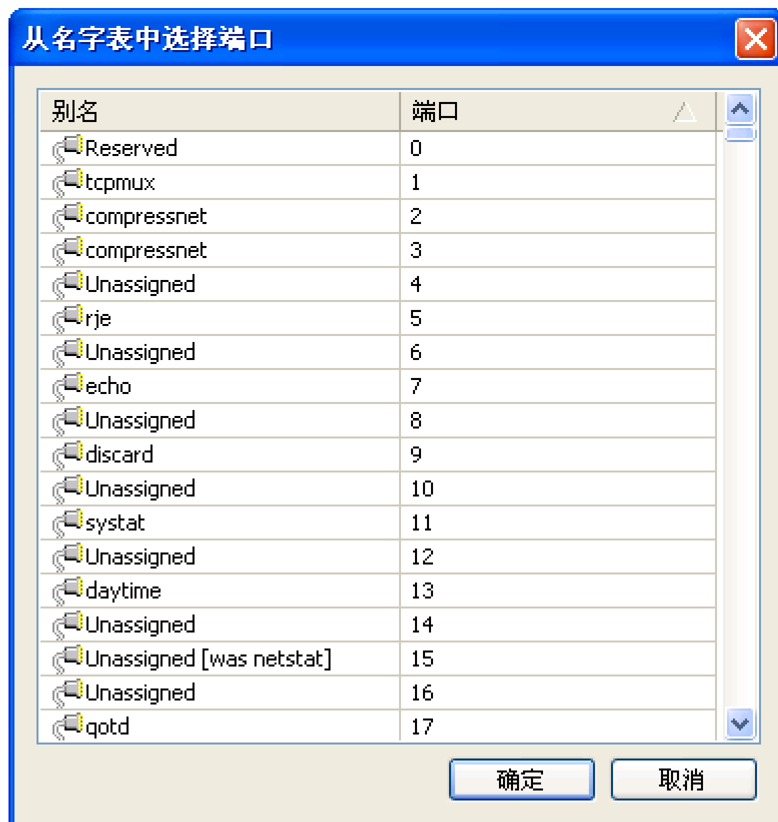
地址过滤

选择地址进行过滤时，你可指定物理地址、IP 地址、IP 范围、IP 掩码来定义双方的地址，同时，也可以对数据包的传输方向做控制，可设定是单向的或是双向的数据。点击▶，也可从“名字表”里面选择物理地址或 IP。点击?图标，可查看地址过滤的格式。

端口过滤

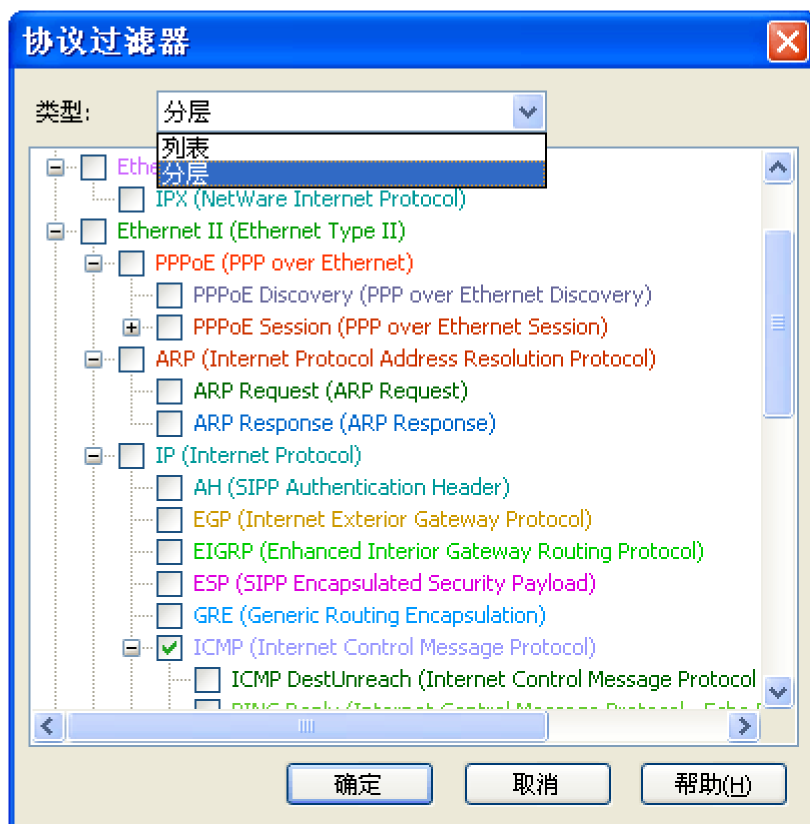
端口过滤也提供多种方式，用户可选择单个端口，也可是一个端口范围，或是多个端口。在选择端口值时，也可以通过名字表，选择 0~48556 的端口值，如下图所示：



协议过滤

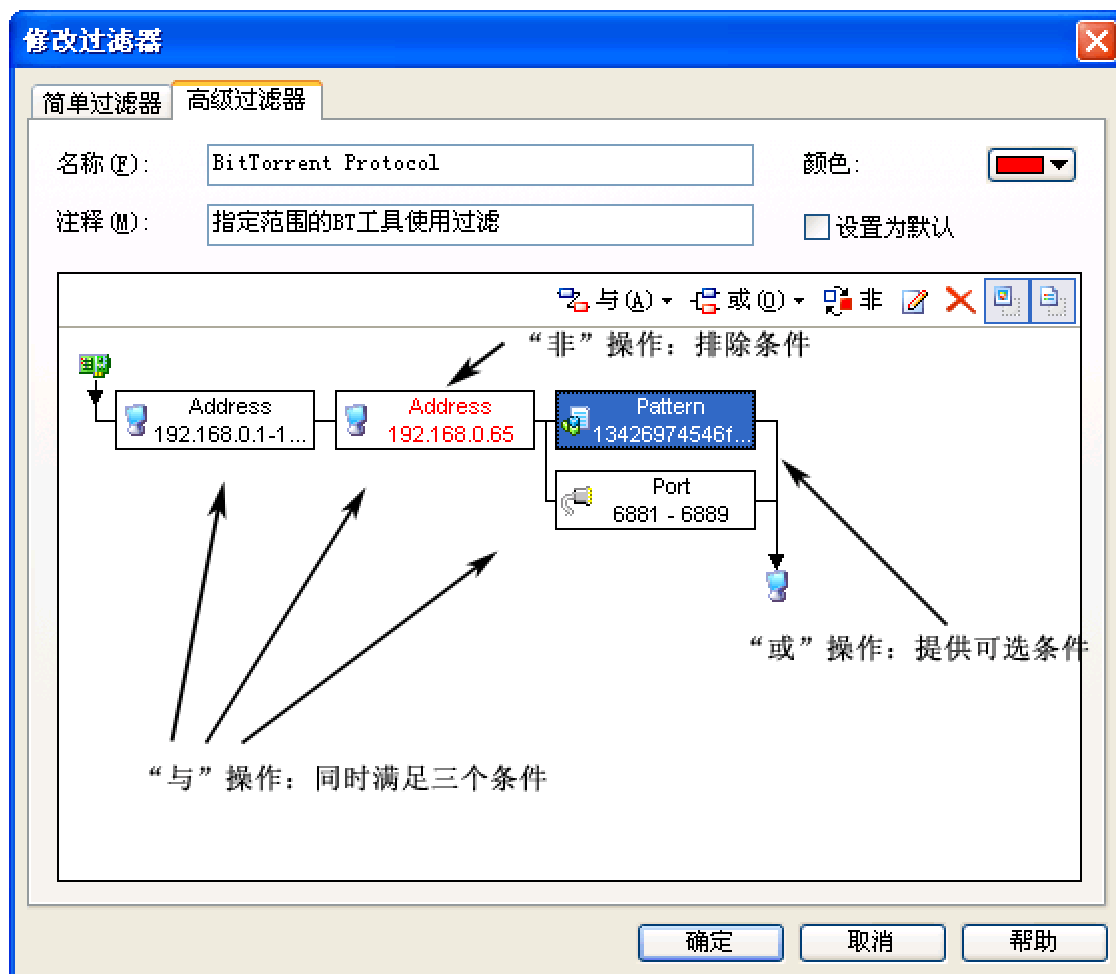
协议过滤提供一个完整的协议树，用户可以选择一种或多种协议来定义过滤条件，如下图所示：



2. 高级过滤

与简单过滤相比，高级过滤增加了“数据包值”筛选、“数据包大小”筛选和“数据包模式配置”筛选条件，并提供多种逻辑关系来组合各种条件。

在高级过滤设置中提供一个非常直观的过滤关系图，图中将展示设定的过滤条件的逻辑关系，通过网卡到主机的过达路径，便可以很轻易看出过滤器的条件关系。



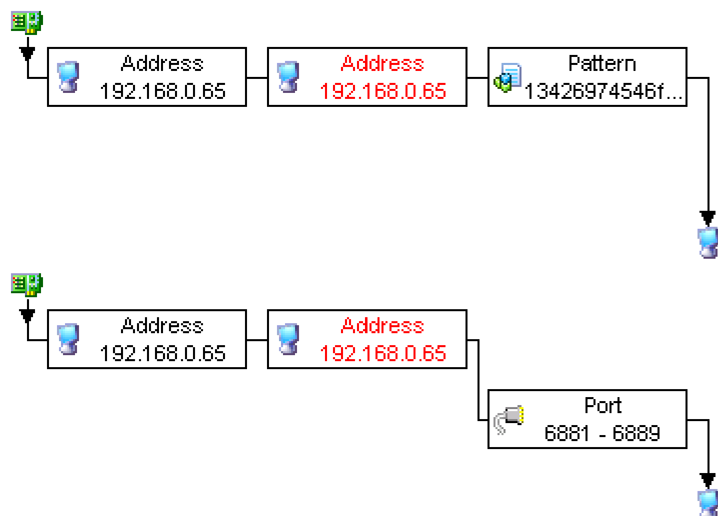
在创建高级过滤器时，可以通过过滤器的工具条组合各种条件，上图是一个监测某段网络范围的 BT 使用过滤设置。

第一个条件：满足一个网段范围，192.168.0.1 - 192.168.0.200

第二个条件：排除一个 IP，192.168.0.65

第三个条件：满足设定的其中一种特征，一个数据包 Hex 值满足“13426974546f7272656e742020726f746f63616c”；或是端口范围是 6881 到 6889 的数据包。

从上图的流程我们可以看出，判断是否是 BT 数据包，看是否满足以下流程：



下面我们来查看一下过滤器工具条：

命令	描述
与(And)	提供“与”关系，必须同时满足关联的两个条件。
或(Or)	提供“或”关系，至少要满足其中一个条件
非(Not)	提供“否”关系，满足的条件与设定的条件相反
Edit	编辑选择的过滤器设置
Delete	删除选择的过滤条件
显示图标	显示过滤器的图标
显示细节	显示过滤器的详细信息

除了包含简单滤过的条件外，高级过滤还可以通过更为精确的条件进行过滤，几乎可以匹配任何条件下的数据包，这些过滤包括：

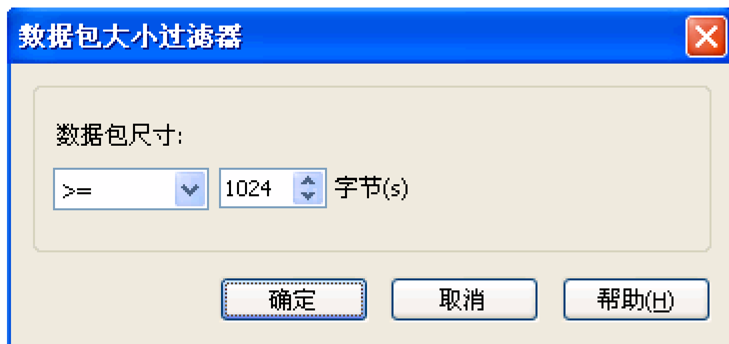
数据包值过滤器

数据包值过滤器

长度: 4 字节
偏移量: 3
掩码: 0xFFFFFFFF
字节序: 网络字序
操作: =
值类型: 无符号十进制
值: 0

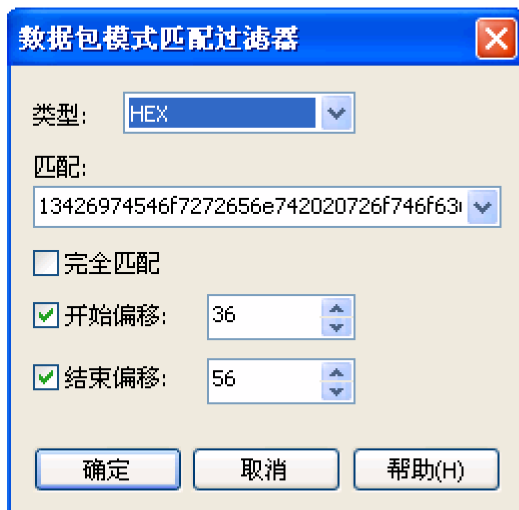
确定
取消
帮助(H)

数据包大小过滤



数据包模式匹配过滤器

下图是一个监测 BT 使用的过滤器。

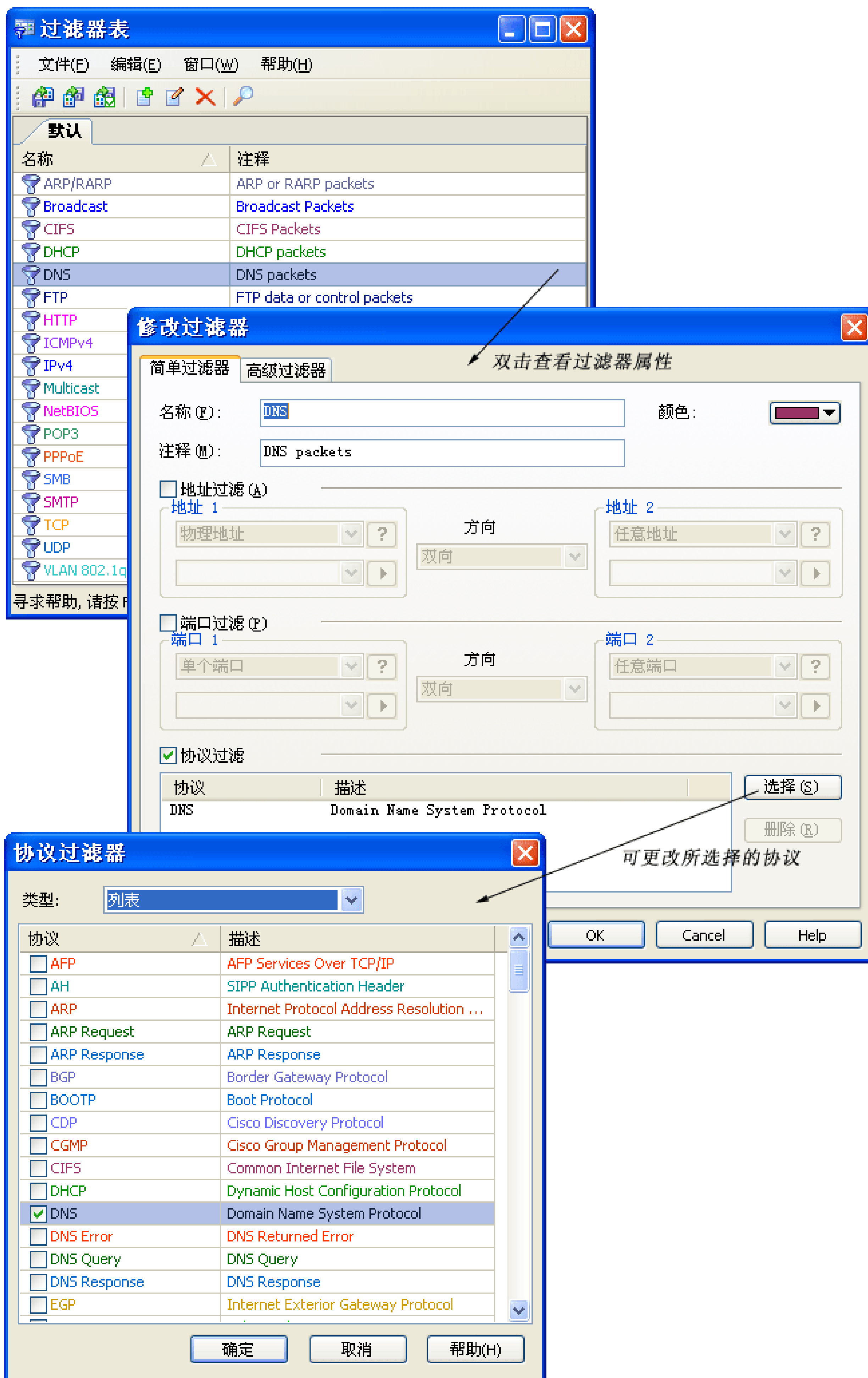


3. 过滤器表

通过点击工具栏上的图标，可以打开过滤器表，可实现对过滤器的管理。

如下图所示，过滤器表里，有系统自带的过滤器，这些默认的过滤器，都属于协议过滤器，是针对协议进行设置的。双击可以打开过滤器的属于对话框，我们可以对过滤器的属于进行修改。包括修改过滤器的名称、注释、颜色，以及过滤器所设置的条件。

下图中，我们选择的是 DNS 过滤器，即所有 DNS 的数据都符合此过滤器的条件。我们通过过滤器条件设置的"选择"选项，便可以通过协议列表，来查看或更改所选择的协议。


过滤器表
文件(F) 编辑(E) 窗口(W) 帮助(H)
默认
名称
注释
ARP/RARP
ARP or RARP packets
Broadcast
Broadcast Packets
CIFS
CIFS Packets
DHCP
DHCP packets
DNS
DNS packets
FTP
FTP data or control packets
HTTP
ICMPv4
IPv4
Multicast
NetBIOS
POP3
PPPoE
SMB
SMTP
TCP
UDP
VLAN 802.1q
修改过滤器
双击查看过滤器属性
简单过滤器
高级过滤器
名称(F):
DNS
颜色:
注释(M):
DNS packets
地址过滤(A)
地址 1
物理地址
方向
双向
地址 2
任意地址
端口过滤(P)
端口 1
单个端口
端口 2
任意端口
协议过滤
协议
描述
DNS
Domain Name System Protocol
选择(S)
删除(R)
可更改所选择的协议
OK
Cancel
Help
协议过滤器
类型:
列表
AFP
AFP Services Over TCP/IP
AH
SIPP Authentication Header
ARP
Internet Protocol Address Resolution ...
ARP Request
ARP Response
BGP
Border Gateway Protocol
BOOTP
Boot Protocol
CDP
Cisco Discovery Protocol
CGMP
Cisco Group Management Protocol
CIFS
Common Internet File System
DHCP
Dynamic Host Configuration Protocol
DNS
Domain Name System Protocol
DNS Error
DNS Returned Error
DNS Query
DNS Response
EGP
Internet Exterior Gateway Protocol
确定
取消
帮助(H)

二十.名字表

科来网络分析系统的名字表可以为网络节点和端口分配常见的、可识别的名称，这些名称可以替代以下各项中的 IP 地址、MAC 地址、端口：

- 节点浏览器
- 端点视图
- 会话视图
- 矩阵视图
- 数据包视图
- 日志视图

你也可以从这些视图中，将 IP 地址，MAC 地址，端口号增加到名字表中。在名字表对话框中，你也可以进行添加、删除和编辑操作。





二十一.命令行

科来网络分析系统 6.4 支持命令行操作，你可以直接在“运行”对话框中输入 capsa 命令启动科来网络分析系统 6.4。

也可以使用 *csnas.exe <.cscproj> | <.cscpkt> | <.cpf> | <.cap> | <.pkt> | <.rawpkt>* 打开一个工程文件或一个数据包文件。

注意：打开的工程文件或数据包文件必须是已经存在的。

Example:

打开 C 盘上的 Traffic056.cscproj 工程文件：在运行窗口中输入“Capsa C:\Traffic056.cscproj”。

通过 C 盘上的 Traffic05624.csctemp 模板文件建立工程：csnas.exe /autostart “C:\Traffic05624.csctemp”。

当不清楚 Capsa 的参数时，可在运行对话框中输入 Capsa /? 命令进行查看。

技术支持部
科来软件
2007 年 4 月